Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0

Manjul Bhargava and Arul Shankar

July 2, 2010

1 Introduction

Any elliptic curve E over $\mathbb{Q}$ is isomorphic to a unique curve of the form $E_{A,B} : y^2 = x^3 + Ax + B$, where $A, B \in \mathbb{Z}$ and for all primes p: $p^6 \nmid B$ whenever $p^4 \mid A$. The (naive) *height* $H(E_{A,B})$ of the elliptic curve $E = E_{A,B}$ is then defined by

$$H(E_{A,B}) := \max\{4|A^3|, 27B^2\}.$$

In a previous paper [7], we showed that the average rank of all elliptic curves, when ordered by their heights, is finite. This was accomplished by proving that the average size of the 2-Selmer group of elliptic curves, when ordered by height, is exactly 3. It then followed from the latter result that the average rank of all elliptic curves is bounded above by 1.5.

In this article, we prove an analogous result for the average size of the 3-Selmer group:

Theorem 1 *When all elliptic curves $E/\mathbb{Q}$ are ordered by height, the average size of the 3-Selmer group $S_3(E)$ is at most 4.*

The above result is also seen to imply the boundedness of the average rank of elliptic curves. Indeed, Theorem 1 immediately yields the following improved bound on the average rank of all elliptic curves:

Corollary 2 *When all elliptic curves over $\mathbb{Q}$ are ordered by height, their average 3-Selmer rank is at most $1\frac{1}{6}$; thus their average rank is also at most $1\frac{1}{6} < 1.17$.*

Theorem 1 also gives the same bound of $1\frac{1}{6}$ on the average 3-rank of the Tate-Shafarevich group of all elliptic curves, when ordered by height.

We will in fact prove a stronger version of Theorem 1, namely:

Theorem 3 *When elliptic curves in any family defined by finitely many local conditions, are ordered by height, the average size of the 3-Selmer group $S_3(E)$ is at most 4.*

Thus the average size of the 3-Selmer group remains at most 4 even when one averages over any subset of elliptic curves defined by finitely many local conditions. We will actually prove Theorem 3 for an even larger class of families, including some that are defined by certain natural infinite sets of local conditions (such as the family of all *semistable* elliptic curves).

Theorem 3, and its above-mentioned extensions, allow us to deduce a number of additional results on ranks that could not be deduced solely through understanding the average size of the 2-Selmer group, as in [7]. First, by combining our counting techniques with the remarkable recent results of Dokchitser–Dokchitser [19] on the parity of p-ranks of Selmer groups, we prove:

Theorem 4 *When all elliptic curves $E/\mathbb{Q}$ are ordered by height, a positive proportion of them have rank* 0.

In the case of rank 1, if we assume the finiteness of the Tate-Shafarevich group, then we also have:

Theorem 5 *Assume $Ш(E)$ is finite for all E. When all elliptic curves $E/\mathbb{Q}$ are ordered by height, a positive proportion of them have rank* 1.

Next, combining our counting arguments with the important recent work of Skinner–Urban [30] on the Iwasawa Main Conjectures for GL_2, we obtain:

Theorem 6 *When all elliptic curves $E/\mathbb{Q}$ are ordered by height, a positive proportion of them have* analytic *rank* 0*; that is, a positive proportion of elliptic curves have nonvanishing* L*-function at $s = 1$.*

As the elliptic curves of analytic rank 0 that arise in Theorem 6 form a subset of those that we construct in Theorem 4, we conclude:

Corollary 7 *A positive proportion of elliptic curves satisfy* BSD.

Our previous results on the average size of the 2-Selmer group were obtained through counting integral binary quartic forms, up to $\mathrm{GL}_2(\mathbb{Z})$-equicalence, having bounded invariants. The connection with elliptic curves is that the process of 2-descent has a classical interpretation in terms of rational binary quartic forms; this connection was indeed behind the beautiful computations of Birch and Swinnerton-Dyer in [8]. The process of 2-descent through the use of binary quartic forms, as in Cremona's remarkable `mwrank` program, remains the fastest method in general for computing ranks of elliptic curves.

In order to prove an analogous upper bound for the average size of 3-Selmer groups, we apply our counting techniques in [7], appropriately modified, to the space $V_{\mathbb{Z}}$ of **integral ternary cubic forms**. The group $\mathrm{SL}_3(\mathbb{Z})$ naturally acts on $V_{\mathbb{Z}}$, and the ring of polynomial invariants for this action turns out to have two independent generators, traditionally denoted I and J, having degrees 4 and 6 respectively.

These invariants may be constructed as follows. For a ternary cubic form f, let $\mathcal{H}(f)$ denote the *Hessian* of f, i.e., the determinant of the 3×3 matrix of second order partial derivatives of f:

$$\mathcal{H}(f(x,y,z)) := \begin{vmatrix} f_{xx} & f_{xy} & f_{xz} \\ f_{xy} & f_{yy} & f_{yz} \\ f_{xz} & f_{yz} & f_{zz} \end{vmatrix}. \tag{1}$$

Then $\mathcal{H}(f)$ is itself a ternary cubic form and, moreover, it is an SL_3-covariant of f, i.e., for $\gamma \in \mathrm{SL}_3(\mathbb{R})$, we have $\mathcal{H}(\gamma \cdot f) = \gamma \cdot \mathcal{H}(f)$. An easy computation gives

$$\mathcal{H}(\mathcal{H}(f)) \;=\; 12288\, I(f)^2 \cdot f \;+\; 512\, J(f) \cdot \mathcal{H}(f) \tag{2}$$

for certain rational polynomials $I(f)$ and $J(f)$ in the coefficients of f, having degrees 4 and 6 respectively; note that (2) uniquely determines $J(f)$, and also uniquely determines $I(f)$ up to sign. The sign of $I(f)$ is fixed by the requirement that the *discriminant* $\Delta(f)$ of a ternary cubic form f be expressible in terms of $I(f)$ and $J(f)$ by the same formula as for binary quartic forms, namely

$$\Delta(f) := \Delta(I,J) := (4I(f)^3 - J(f)^2)/27. \tag{3}$$

These polynomials $I(f)$ and $J(f)$ are evidently $\mathrm{SL}_3(\mathbb{Z})$-invariant, and in fact they generate the full ring of polynomial invariants over $\mathbb{C}$ (see, e.g., [31]).

Now, for ternary cubic forms over the integers, the general work of Borel and Harish-Chandra [9] implies that the number of equivalence classes of integral ternary cubic forms, having any given fixed values for these basic invariants I and J (so long as I and J are not both equal to zero), is finite. The question thus arises: how many $\mathrm{SL}_3(\mathbb{Z})$-classes of integral ternary cubic forms are there, on average, having invariants I, J, as the pair (I, J) varies?

To answer this question, we require a couple of definitions. Let us define the *height* of a ternary cubic form $f(x, y, z)$ by

$$H(f) := H(I, J) := \max\{|I^3|, J^2/4\}$$

(as usual, the constant factor $1/4$ on J^2 is present for convenience and is not of any real importance). Thus $H(f)$ is a "degree 12" function on the coefficients of f. We may then order all $\mathrm{SL}_3(\mathbb{Z})$-classes of ternary cubic forms f by their height $H(f)$, and we may order all pairs (I, J) of invariants by their height $H(I, J)$.

As with binary quartic forms, we wish to restrict ourselves to counting ternary cubic forms that are irreducible in an appropriate sense. Being simply *irreducible*—i.e., not having a smaller degree factor—is more a geometric condition rather than an arithmetic one. We wish to have a condition that implies that the ternary cubic form is sufficiently "generic" over $\mathbb{Q}$. The most convenient notion (also for the applications) turns out to be what we call strong irreducibility.

Let us say that an integral ternary cubic form is *strongly irreducible* if the common zero set of f and its Hessian $\mathcal{H}(f)$ in $\mathbb{P}^2$ (i.e., the set of *flexes* of f in $\mathbb{P}^2$) contains no rational points. (Note that this implies that f is *irreducible* in the usual sense, i.e., it does not factor over $\mathbb{Q}$). We prove:

Theorem 8 *Let $h(I, J)$ denote the number of $\mathrm{SL}_3(\mathbb{Z})$-equivalence classes of strongly irreducible ternary cubic forms having invariants equal to I and J. Then:*

$$\text{(a)} \quad \sum_{\substack{\Delta(I,J)>0 \\ H(I,J)<X}} h(I, J) \;=\; \frac{32}{45}\zeta(2)\zeta(3) \cdot X^{5/6} \;+\; o(X^{5/6});$$

$$\text{(b)} \quad \sum_{\substack{\Delta(I,J)<0 \\ H(I,J)<X}} h(I, J) \;=\; \frac{128}{45}\zeta(2)\zeta(3) \cdot X^{5/6} \;+\; o(X^{5/6}).$$

In order to obtain the average size of $h(I, J)$, as (I, J) varies, we first need to know which pairs (I, J) can actually occur as the invariants of an integral ternary quartic form. For example, in the case of binary quadratic and binary cubic forms, the answer is well-known: there is only one invariant—the *discriminant*—and a number occurs as the discriminant of a binary quadratic (resp. cubic) form if and only if it is congruent to 0 or 1 (mod 4).

In the binary quartic case, we proved in [7] that a similar scenario occurs; namely, an $(I, J) \in \mathbb{Z} \times \mathbb{Z}$ is *eligible*—i.e., it occurs as the invariants of some integer binary quartic form—if and only if it satisfies any one of a certain specified finite set of congruence conditions modulo 27 (see [7, Theorem 1.7]).

It turns out that the invariants (I, J) that can occur (i.e., are *eligible*) for an integral ternary cubic must also satisfy these same conditions modulo 27. However, there is also now a strictly larger set of possibilities at the prime 2. Indeed, the pairs (I, J) that occur for ternary cubic forms need

not even be integral, but rather lie in $\frac{1}{16}\mathbb{Z} \times \frac{1}{32}\mathbb{Z}$; and the pairs (I, J) in this set that actually occur are then defined by certain congruence conditions modulo 64 on $16I$ and $32J$, in addition to the same congruence conditions modulo 27 on I and J that occur for binary quartic forms.

In particular, the set of integral pairs $(I, J) \in \mathbb{Z} \times \mathbb{Z}$ that occur as invariants for integral ternary cubic forms is the same as the set of all pairs (I, J) that occur for integral binary quartic forms! We prove:

Theorem 9 *A pair (I, J) occurs as the pair of invariants of an integral ternary cubic form if and only if $(I, J) \in \frac{1}{16}\mathbb{Z} \times \frac{1}{32}\mathbb{Z}$, the pair $(16I, 32J)$ satisfies one of the following congruence conditions modulo 64:*

(a) $16I \equiv 0 \pmod{16}$ *and* $32J \equiv 0 \pmod{32}$, (f) $16I \equiv 25 \pmod{64}$ *and* $32J \equiv 3 \pmod{32}$,

(b) $16I \equiv 0 \pmod{16}$ *and* $32J \equiv 8 \pmod{32}$, (g) $16I \equiv 33 \pmod{64}$ *and* $32J \equiv 15 \pmod{32}$,

(c) $16I \equiv 1 \pmod{64}$ *and* $32J \equiv 31 \pmod{32}$, (h) $16I \equiv 41 \pmod{64}$ *and* $32J \equiv 11 \pmod{32}$,

(d) $16I \equiv 9 \pmod{64}$ *and* $32J \equiv 27 \pmod{32}$, (i) $16I \equiv 49 \pmod{64}$ *and* $32J \equiv 23 \pmod{32}$,

(e) $16I \equiv 17 \pmod{64}$ *and* $32J \equiv 7 \pmod{32}$, (j) $16I \equiv 57 \pmod{64}$ *and* $32J \equiv 19 \pmod{32}$,

and (I, J) satisfies one of the following congruence conditions modulo 27:

(a) $I \equiv 0 \pmod{3}$ *and* $J \equiv 0 \pmod{27}$,

(b) $I \equiv 1 \pmod{9}$ *and* $J \equiv \pm 2 \pmod{27}$,

(c) $I \equiv 4 \pmod{9}$ *and* $J \equiv \pm 16 \pmod{27}$,

(d) $I \equiv 7 \pmod{9}$ *and* $J \equiv \pm 7 \pmod{27}$.

From Theorem 9, we conclude that the number of eligible pairs $(I, J) \in \frac{1}{16}\mathbb{Z} \times \frac{1}{32}\mathbb{Z}$, with $H(I, J) < X$, is a certain constant times $X^{5/6}$; by Theorem 8, the number of classes of strongly irreducible ternary cubic forms, per eligible $(I, J) \in \frac{1}{16}\mathbb{Z} \times \frac{1}{32}\mathbb{Z}$, is therefore a constant on average. We have:

Theorem 10 *Let $h(I, J)$ denote the number of $\mathrm{SL}_3(\mathbb{Z})$-equivalence classes of strongly irreducible integral ternary cubic forms having invariants equal to I and J. Then:*

$$\text{(a)} \lim_{X\to\infty} \frac{\sum\limits_{\substack{\Delta(I,J)>0 \\ H(I,J)<X}} h(I,J)}{\sum\limits_{\substack{(I,J) \text{ eligible} \\ \Delta(I,J)>0 \\ H(I,J)<X}} 1} = 3\zeta(2)\zeta(3); \qquad \text{(b)} \lim_{X\to\infty} \frac{\sum\limits_{\substack{\Delta(I,J)<0 \\ H(I,J)<X}} h(I,J)}{\sum\limits_{\substack{(I,J) \text{ eligible} \\ \Delta(I,J)<0 \\ H(I,J)<X}} 1} = 3\zeta(2)\zeta(3).$$

The fact that this *class number* $h(I, J)$ is a finite constant on average is indeed what allows us to show that the size of the 3-Selmer group of elliptic curves too is bounded by a finite constant on average.

We actually prove a strengthening of Theorem 10; namely, we obtain the asymptotic count of ternary cubic forms having bounded invariants that satisfy any specified finite set of congruence conditions (see §2.4, Theorem 20). This strengthening turns out to be crucial for the application to 3-Selmer groups (as in Theorem 1), as we now discuss.

Recall that, for any positive integer n, an element of the n-Selmer group $S_n(E)$ of an elliptic curve $E/\mathbb{Q}$ may be thought of as a locally soluble n-covering. An *n-covering* of $E/\mathbb{Q}$ is a genus one curve C together with maps $\phi : C \to E$ and $\theta : C \to E$, where ϕ is an isomorphism defined over $\mathbb{C}$, and θ is a degree n^2 map defined over $\mathbb{Q}$ such that the following diagram commutes:

$$\begin{array}{ccc} E & \xrightarrow{[n]} & E \\ {\scriptstyle\phi}\uparrow & \nearrow_{\theta} & \\ C & & \end{array}$$

Thus an n-covering $C = (C, \phi, \theta)$ may be viewed as a "twist over $\mathbb{Q}$ of the multiplication-by-n map on E". Two n-coverings C and C' are said to be *isomorphic* if there exists an isomorphism $\Phi : C \to C'$ defined over $\mathbb{Q}$, and an n-torsion point $P \in E$, such that the following diagram commutes:

$$\begin{array}{ccc} E & \xrightarrow{+P} & E \\ {\scriptstyle\phi}\uparrow & & \uparrow{\scriptstyle\phi'} \\ C & \xrightarrow[\Phi]{} & C' \end{array}$$

A *soluble n-covering* C is one that possesses a rational point, while a *locally soluble n-covering* C is one that possesses an $\mathbb{R}$-point and a $\mathbb{Q}_p$-point for all primes p. Then we have, as groups, the isomorphisms:

$$\begin{aligned} \{\text{soluble } n\text{-coverings}\}/\sim &\cong E(\mathbb{Q})/nE(\mathbb{Q}); \\ \{\text{locally soluble } n\text{-coverings}\}/\sim &\cong S_n(E). \end{aligned}$$

Now, counting elements of $S_3(E)$ leads to counting ternary cubic forms for the following reason. There is a result of Cassels (see [12, Theorem 1.3]) that states that any locally soluble n-covering C posseses a degree n divisor defined over $\mathbb{Q}$. If $n = 3$, we thus obtain an embedding of C into $\mathbb{P}^2$, thereby yielding a ternary cubic form, well-defined up to $\mathrm{GL}_3(\mathbb{Q})$-equivalence! Conversely, given any ternary cubic form f having rational coefficients and nonzero discriminant, there exists a degree 9 mapping defined over $\mathbb{Q}$ from the plane cubic C defined by the equation $f = 0$ to the elliptic curve $\mathrm{Jac}(C)$, where $\mathrm{Jac}(C)$ is the Jacobian of C and is given by the equation

$$Y^2 = X^3 - \frac{I(f)}{3}X - \frac{J(f)}{27}. \tag{4}$$

Note that (4) gives another nice interpretation for the invariants $I(f)$ and $J(f)$ of a ternary cubic form f.

To carry out the proof of Theorems 1 and 3, we do the following:

- Given $A, B \in \mathbb{Z}$, choose an *integral* ternary cubic form f for each element of $S_3(E_{A,B})$, such that
  - $f(x, y, z)$ gives the desired 3-covering;
  - the invariants $(I(f), J(f))$ of f agree with the invariants (A, B) of the elliptic curve (at least away from 2 and 3);

- Count these integral ternary cubic forms via Theorem 11. The relevant ternary cubic forms are defined by infinitely many congruence conditions, so a suitable sieve has to be performed.

As we are primarily aiming for upper bounds, we are able to use a particularly simple sieve in the last step (compare with [7]) in order to prove Theorems 1 and 3.

This paper is organized as follows. In Section 2, following the methods of [7], we determine the asymptotic number of $\mathrm{SL}_3(\mathbb{Z})$-equivalence classes of strongly irreducible integral ternary cubic forms having bounded height; in particular, we prove Theorems 8, 9, and 10. The primary method is that of reduction theory, allowing us to reduce the problem to counting integral points in certain finite volume regions in $\mathbb{R}^{10}$. However, the difficulty in such a count, as usual, lies in the fact that these regions are not compact, but rather have cusps going off to infinity. By studying the geometry of these regions via the averaging method of [7], we are able to cut down to the subregions of the fundamental domains that contain predominantly and all of the strongly irreducible points. The appropriate volume computations for these subregions are then carried out to obtain the desired result.

In Section 3, we then describe the precise correspondence between ternary cubic forms and elements in the 3-Selmer groups of elliptic curves. We show, in particular, that non-identity elements of the 3-Selmer group correspond to strongly irreducible ternary cubic forms. We then apply this correspondence, together with the counting results of Section 2 and a simple sieve (which involves the determination of certain local mass formulae for 3-coverings of elliptic curves over $\mathbb{Q}_p$), to prove that the average size of the 3-Selmer groups of elliptic curves, when ordered by height, is at most 4; we thus prove Theorems 1 and 3.

Finally, in Section 4, we combine the results of Sections 2 and 3, as well as the aforementioned results of Dokchitser–Dokchitser [19] and Skinner–Urban [30], to obtain Theorems 4, 5, and 6.

2 The number of integral ternary cubic forms having bounded invariants

Let $V_{\mathbb{R}}$ denote the space of all ternary cubic forms having coefficients in $\mathbb{R}$. The group $\mathrm{GL}_3(\mathbb{R})$ acts on $V_{\mathbb{R}}$ on the left via linear substitution of variable; namely, if $\gamma \in \mathrm{GL}_3(\mathbb{R})$ and $f \in V_{\mathbb{R}}$, then

$$(\gamma \cdot f)(x, y, z) = f((x, y, z) \cdot \gamma).$$

For a ternary cubic form $f \in V_{\mathbb{R}}$, let $\mathcal{H}(f)$ denote the Hessian covariant of f, defined by (1), and let $I(f)$ and $J(f)$ denote the two fundamental polynomial invariants of f as in (2). As noted earlier, these polynomials $I(f)$ and $J(f)$ are invariant under the action of $\mathrm{SL}_3(\mathbb{R}) \subset \mathrm{GL}_3(\mathbb{R})$ and, moreover, they are *relative invariants* of degrees 4 and 6, respectively, for the action of $\mathrm{GL}_3(\mathbb{R})$ on $V_{\mathbb{R}}$; i.e, $I(\gamma \cdot f) = \det(\gamma)^4 I(f)$ and $J(\gamma \cdot f) = \det(\gamma)^6 J(f)$ for $\gamma \in \mathrm{GL}_3(\mathbb{R})$ and $f \in V_{\mathbb{R}}$.

The discriminant $\Delta(f)$ of a ternary cubic form f is a relative invariant of degree 12, as may be seen by the formula $\Delta(f) = \Delta(I, J) = (4I(f)^3 - J(f)^2)/27$. We define the *height* $H(f)$ of f by

$$H(f) := H(I, J) := \max(|I(f)|^3, J(f)^2/4).$$

Note that the height is also a degree 12 relative invariant for the action of $\mathrm{GL}_3(\mathbb{R})$ on $V_{\mathbb{R}}$.

It is easy to see that the action of $\mathrm{SL}_3(\mathbb{Z}) \subset \mathrm{GL}_3(\mathbb{R})$ on $V_{\mathbb{R}}$ preserves the lattice $V_{\mathbb{Z}}$ consisting of integral ternary cubic forms. In fact, it also preserves the two sets $V_{\mathbb{Z}}^+$ and $V_{\mathbb{Z}}^-$ consisting of those integral ternary cubics that have positive and negative discriminant, respectively.

As before, let us say that an integral ternary cubic form is *strongly irreducible* if the corresponding cubic curve in $\mathbb{P}^2$ has no rational flex. Our purpose in this section is to prove the following restatement of Theorem 8:

Theorem 11 *For an* $\mathrm{SL}_3(\mathbb{Z})$*-invariant set* $S \subset V_{\mathbb{Z}}$*, let* $N(S;X)$ *denote the number of* $\mathrm{SL}_3(\mathbb{Z})$*-equivalence classes of strongly irreducible elements in* S *having height bounded by* X*. Then*

(a) $N(V_{\mathbb{Z}}^+;X) = \dfrac{32}{45}\,\zeta(2)\zeta(3)X^{5/6} + o(X^{5/6})$;

(b) $N(V_{\mathbb{Z}}^-;X) = \dfrac{128}{45}\zeta(2)\zeta(3)X^{5/6} + o(X^{5/6})$.

2.1 Reduction theory

Let $V_{\mathbb{R}}^+$ (resp. $V_{\mathbb{R}}^-$) denote the set of elements in $V_{\mathbb{R}}$ having positive (resp. negative) discriminant. We first construct fundamental sets in $V_{\mathbb{R}}^{\pm}$ for the action of $\mathrm{GL}_3^+(\mathbb{R})$ on $V_{\mathbb{R}}^{\pm}$, where $\mathrm{GL}_3^+(\mathbb{R})$ is the subgroup of all elements in $\mathrm{GL}_3(\mathbb{R})$ having positive determinant.

To this end, let f be a ternary cubic form in $V_{\mathbb{R}}^{\pm}$ having nonzero discriminant, and let C denote the cubic curve in $\mathbb{P}^2$ defined by the equation $f(x,y,z)=0$. The set of flexes of C is given by the set of common zeroes of f and $\mathcal{H}(f)$ in $\mathbb{P}^2$, and hence the number of such flexes is 9 by Bezout's Theorem. As both f and $\mathcal{H}(f)$ have real coefficients, the flex points of C are either real or come in complex conjugate pairs. Therefore, since the total number of flex points is odd, C possesses at least one real flex point.

This implies, in particular, that any ternary cubic form over $\mathbb{R}$ is $\mathrm{SL}_3(\mathbb{R})$-equivalent to one in Weierstrass form, i.e., one in the form

$$f(x,y,z) = x^3 + Axz^2 + Bz^3 - y^2z \tag{5}$$

for some $A, B \in \mathbb{R}$. It can be checked that the ternary cubic form f in (5) has invariants $I(f)$ and $J(f)$ equal to $-3A$ and $-27B$, respectively. Thus, since I and J are relative invariants of degrees 4 and 6, respectively, two ternary cubic forms f and g over $\mathbb{R}$ are $\mathrm{GL}_3^+(\mathbb{R})$-equivalent if and only if there exists a positive constant $\lambda \in \mathbb{R}$ such that $I(f) = \lambda^4 I(g)$ and $J(f) = \lambda^6 J(g)$. It follows that a fundamental set L^+ (resp. L^-) for the action of $\mathrm{GL}_3^+(\mathbb{R})$ on $V_{\mathbb{R}}^+$ (resp. $V_{\mathbb{R}}^-$) may be constructed by choosing one ternary cubic form for each I and J such that $H(I,J)=1$ and $4I^3 - J^2 > 0$ (resp. $4I^3 - J^2 < 0$). We may thus choose

$$\begin{aligned} L^+ &= \Big\{x^3 - \frac{1}{3}xz^2 - \frac{J}{27}z^3 - y^2z : -2 \le J \le 2\Big\} \\ L^- &= \Big\{x^3 - \frac{I}{3}xz^2 \pm \frac{2}{27}z^3 - yz^2 : -1 \le I \le 1\Big\} \cup \Big\{x^3 + \frac{1}{3}xz^2 - \frac{J}{27}z^3 - yz^2 : -2 \le J \le 2\Big\}. \end{aligned}$$

The key fact that we will need about these fundamental sets $L^{\pm}$ is that the coefficients of all the ternary cubic forms in the $L^{\pm}$ are uniformly bounded. Note also that if $G_0 \subset \mathrm{GL}_3^+(\mathbb{R})$ is any fixed compact subset then, for any $h \in G_0$, the set $hL^{\pm}$ is also a fundamental set for the action of $\mathrm{GL}_3^+(\mathbb{R})$ on $V_{\mathbb{Z}}^{\pm}$, and again the coefficients of all the forms in $hL^{\pm}$ are uniformly bounded, independent of $h \in G_0$.

We also require the following fact whose proof we postpone to Section 3:

Lemma 12 *Let* $f \in V_{\mathbb{R}}$ *be any ternary cubic form having nonzero discriminant. Then the size of the stabilizer in* $\mathrm{GL}_3^+(\mathbb{R})$ *of* f *is equal to* 3*.*

Let $\mathcal{F}$ denote a fundamental domain in $\mathrm{GL}_3(\mathbb{R})$ for the left action of $\mathrm{GL}_3^+(\mathbb{Z}) = \mathrm{SL}_3(\mathbb{Z})$ on $\mathrm{GL}_3^+(\mathbb{R})$ that is contained in a standard Siegel set. We may assume that $\mathcal{F} = \{nak\lambda : n \in N'(a),\, a \in A',\, k \in K,\, \lambda \in \Lambda\}$, where

$$\begin{aligned}
K &= \text{subgroup } \mathrm{SO}_3(\mathbb{R}) \subset \mathrm{GL}_3^+(\mathbb{R}) \text{ of orthogonal transformations;} \\
A' &= \{a(s_1,s_2) : s_1, s_2 > c\}, \\
&\qquad \text{where } a(s_1,s_2) = \begin{pmatrix} s_1^{-2}s_2^{-1} & & \\ & s_1 s_2^{-1} & \\ & & s_1 s_2^2 \end{pmatrix}; \\
N' &= \{n(u_1,u_2,u_3) : (u_1,u_2,u_3) \in \nu(a)\}, \\
&\qquad \text{where } n(u_1,u_2,u_3) = \begin{pmatrix} 1 & & \\ u_1 & 1 & \\ u_2 & u_3 & 1 \end{pmatrix}; \\
\Lambda &= \{\lambda : \lambda > 0\}, \\
&\qquad \text{where } \lambda = \begin{pmatrix} \lambda & & \\ & \lambda & \\ & & \lambda \end{pmatrix};
\end{aligned}$$

here $\nu(a)$ is a measurable subset of $[-1/2,1/2]^3$ dependent only on $a \in A'$ and $c > 0$ is an absolute constant.

We see from Lemma 12 that for any $g \in \mathrm{GL}_3^+(\mathbb{R})$, the multiset $\mathcal{F}gL^{\pm}$ is essentially the union of 3 fundamental domains for the action of $\mathrm{SL}_3(\mathbb{Z})$ on $V_{\mathbb{R}}^{\pm}$. More precisely, we see that an $\mathrm{SL}_3(\mathbb{Z})$-equivalence class of $x \in V_{\mathbb{R}}^{\pm}$ is represented exactly $m(x)$ times in $\mathcal{F}gL^{\pm}$, where $m(x) = \#\mathrm{Stab}_{\mathrm{SL}_3(\mathbb{R})}(x)/\#\mathrm{Stab}_{\mathrm{SL}_3(\mathbb{Z})}(x)$.

However, let us say that a ternary cubic form $f \in V_{\mathbb{Z}}$ is *totally irreducible* if it is strongly irreducible and its Jacobian (i.e., the Jacobian of the plane cubic curve associated to f) does not possess a nontrivial rational 3-torsion point. Then we have the following fact, whose proof will be given in Section 3.

Lemma 13 *The stabilizer in* $\mathrm{SL}_3(\mathbb{Z})$ *of a totally irreducible integral ternary cubic form* $f \in V_{\mathbb{Z}}$ *is trivial.*

Furthermore, we will also prove in §2.5 that the number of $\mathrm{SL}_3(\mathbb{Z})$-orbits of points in $V_{\mathbb{Z}}$ that are strongly irreducible but not totally irreducible, and have height less than X, is negligible (i.e., $o(X^{5/6})$).

For $h \in \mathrm{GL}_3^+(\mathbb{R})$, let $\mathcal{R}_X(L^+,h)$ and $\mathcal{R}_X(L^-,h)$ denote the multisets defined by

$$\mathcal{R}_X(L^{\pm},h) := \{f \in \mathcal{F}hL^{\pm} : H(f) < X\}.$$

Then by Lemmas 12 and 13, that we see that, up to a negligible number of forms that are not totally irreducible, the quantity $3 \cdot N(V_{\mathbb{Z}}^{\pm}; X)$ is equal to the number of strongly irreducible integral ternary cubic forms contained in $\mathcal{R}_X(L^{\pm},h)$.

Counting strongly irreducible integer points in a single such $\mathcal{R}_X(L^{\pm},h)$ is difficult because the domain $\mathcal{R}_X(L^{\pm},h)$ is not compact. As in [7], we simplify the counting by averaging over lots of such domains, i.e., by averaging over a continuous range of elements h lying in a certain fixed compact subset of $\mathrm{GL}_3^+(\mathbb{R})$.

2.2 Averaging and cutting off the cusp

Let $G_0 \subset \mathrm{GL}_3^+(\mathbb{R})$ be a compact K-invariant subset that is the closure of some nonempty open set in $\mathrm{GL}_3^+(\mathbb{R})$, such that every element in G_0 has determinant greater than 1. For any $\mathrm{SL}_3(\mathbb{Z})$-invariant set $S \subset V_{\mathbb{Z}}^{\pm}$, let S^{irr} denote the set of strongly irreducible elements of S. Then, up to an error of $o(X^{5/6})$ from the bound (proved in Lemma 22) on points that are strongly but not totally irreducible, we have:

$$N(S;X) = \frac{\int_{h\in G_0} \#\{x \in \mathcal{R}_X(L,h) \cap S^{\mathrm{irr}}\}dh}{C_{G_0}}, \tag{6}$$

where $L = L^{\pm}$ and $C_{G_0} = 3\int_{h\in G_0} dh$. Given $x \in V_{\mathbb{Z}}^{\pm}$, let x_L denote the unique point in L that is $\mathrm{GL}_3^+(\mathbb{R})$-equivalent to x. Then we have

$$N(S;X) = \frac{1}{C_{G_0}} \sum_{\substack{x\in S^{\mathrm{irr}} \\ H(x)<X}} \int_{h\in G_0} \#\{g \in \mathcal{F} : x = ghx_L\}dh. \tag{7}$$

For a given $x \in S^{\mathrm{irr}}$, by Lemma 12 there exist three elements g_1, g_2, $g_3 \in \mathrm{GL}_3^+(\mathbb{R})$ satisfying $g_i x_L = x$. Hence

$$\int_{h\in G_0} \#\{g \in \mathcal{F} : x = ghx_L\}dh \;=\; \sum_{i=1}^{3} \int_{h\in G_0} \#\{g \in \mathcal{F} : gh = g_i\}dh \;=\; \sum_{i=1}^{3} \int_{h\in G_0\cap \mathcal{F}^{-1}g_i} dh.$$

Since dh is an invariant measure on $\mathrm{GL}_3^+(\mathbb{R})$, we see that

$$\sum_{i=1}^{3} \int_{h\in G_0\cap \mathcal{F}^{-1}g_i} dh = \sum_{i=1}^{3} \int_{g\in G_0 g_i^{-1}\cap \mathcal{F}^{-1}} dg = \sum_{i=1}^{3} \int_{g\in\mathcal{F}} \#\{h \in G_0 : gh = g_i\}dg = \int_{g\in\mathcal{F}} \#\{h \in G_0 : x = ghx_L\}dg.$$

Therefore, if $d^\times s := d^\times s_1 d^\times s_2$, then

$$\begin{aligned}
N(S;X) \;&=\; \frac{1}{C_{G_0}} \sum_{\substack{x\in S^{\mathrm{irr}} \\ H(x)<X}} \int_{g\in\mathcal{F}} \#\{h \in G_0 : x = ghx_L\}dg. && (8)\\
&=\; \frac{1}{C_{G_0}} \int_{g\in\mathcal{F}} \#\{x \in S^{\mathrm{irr}} \cap gG_0L : H(x) < X\}\, dg && (9)\\
&=\; \frac{1}{C_{G_0}} \int_{g\in N'(a)A'\Lambda K} \#\{x \in S^{\mathrm{irr}} \cap na(s_1,s_2)\lambda kG_0L : H(x) < X\} s_1^{-6}s_2^{-6} dn\, d^\times s\, d^\times\lambda\, dk && (10)\\
&=\; \frac{1}{C_{G_0}} \int_{g\in N'(a)A'\Lambda} \#\{x \in S^{\mathrm{irr}} \cap na(s_1,s_2)\lambda G_0L : H(x) < X\} s_1^{-6}s_2^{-6} dn\, d^\times s\, d^\times\lambda\,, && (11)
\end{aligned}$$

where the last equality follows because we have assumed that G_0 is K-invariant and $\int_K dk = 1$.

For $na(s_1,s_2)\lambda \in \mathcal{F}$, let us write $B(n,s_1,s_2,\lambda,X) := \{x \in na(s_1,s_2)\lambda G_0L : H(x) < X\}$. We then have

$$N(S;X) = \frac{1}{C_{G_0}} \int_{g\in N'(a)A'\Lambda} \#\{x \in S^{\mathrm{irr}} \cap B(n,s_1,s_2,\lambda,X)\} s_1^{-6}s_2^{-6} dn\, d^\times t\, d^\times\lambda\,. \tag{12}$$

To further simplify the right hand side of (12), we require the following lemma which states that $B(n, s_1, s_2, \lambda, X)$ contains no strongly irreducible points if s_1 or s_2 is large enough (i.e., when we are in the "cuspidal regions" of the fundamental domains):

Lemma 14 *Let $C > 1$ be a constant that bounds the absolute values of the x^3, x^2y, xy^2, and x^2z coefficients of all the forms in $G_0L^{\pm}$. Then the set $B(n, s_1, s_2, \lambda, X)$ contains no strongly irreducible integral ternary cubic forms if $s_1 > 3C\lambda/c^3$ or if $s_2 > 3C\lambda/c^3$.*

Proof: It is easy to see that if $s_1 > 3C\lambda/c^3$, then the absolute values of the coefficients of x^3, x^2y, and x^2z of any ternary cubic form in $B(n, s_1, s_2, \lambda, X)$ are all less than 1. Therefore any integral ternary cubic form in $B(n, s_1, s_2, \lambda, X)$ must have its x^3, x^2y, and x^2z coefficients equal to 0, and such a form has a rational flex at $[1, 0, 0] \in \mathbb{P}^2$ and so is not strongly irreducible.

Similarly, if $s_2 > 3C\lambda/c^3$, then any integral ternary cubic form in $B(n, s_1, s_2, \lambda, X)$ has its x^3, x^2y, and xy^2 coefficients equal to 0, and such a form too always has a flex at $[1, 0, 0] \in \mathbb{P}^2$, and so is not strongly irreducible. □

Now let $V_{\mathbb{Z}}^{\mathrm{red}}$ denote the set of all integral ternary cubic forms that are not totally irreducible. Then we have the following lemma which states that the number of reducible points—i.e., points in $V_{\mathbb{Z}}^{\mathrm{red}}$—that are in the "main body" of the fundamental domains is negligible.

Lemma 15 *Let $\mathcal{F}'$ denote the set of elements $na(s_1, s_2)\lambda k \in \mathcal{F}$ that satisfy $s_1 < 3C\lambda/c^3$ and $s_2 < 3C\lambda/c^3$. Then*

$$\int_{na(s_1,s_2)\lambda k \in \mathcal{F}'} \#\{x \in V_{\mathbb{Z}}^{\mathrm{red}} \cap B(n, s_1, s_2, \lambda, X)\} s_1^{-6} s_2^{-6} dn\, d^{\times}t\, d^{\times}\lambda dk = o(X^{5/6}).$$

We defer the proof of Lemma 15 to Section 2.6.

To estimate the number of integral ternary cubic forms in $B(n, s_1, s_2, \lambda, X)$, we use the following proposition due to Davenport [15].

Proposition 16 *Let $\mathcal{R}$ be a bounded, semi-algebraic multiset in $\mathbb{R}^n$ having maximum multiplicity m, and that is defined by at most k polynomial inequalities each having degree at most ℓ. Let $\mathcal{R}'$ denote the image of $\mathcal{R}$ under any (upper or lower) triangular, unipotent transformation of $\mathbb{R}^n$. Then the number of integer lattice points (counted with multiplicity) contained in the region $\mathcal{R}'$ is*

$$\mathrm{Vol}(\mathcal{R}) + O(\max\{\mathrm{Vol}(\bar{\mathcal{R}}), 1\}),$$

where $\mathrm{Vol}(\bar{\mathcal{R}})$ denotes the greatest d-dimensional volume of any projection of $\mathcal{R}$ onto a coordinate subspace obtained by equating $n - d$ coordinates to zero, where d takes all values from 1 to $n - 1$. The implied constant in the second summand depends only on n, m, k, and ℓ.

Therefore, by Equation (12), Lemmas 14 and 15, and Proposition 16, we see that up to an error of $o(X^{5/6})$, we have

$$N(V_{\mathbb{Z}}^{\pm}; X) = \int_{na(s_1,s_2)\lambda k \in \mathcal{F}'} \big(\mathrm{Vol}(B(n, s_1, s_2, \lambda, X)) + O(\lambda^{24} s_1^6 s_2^3)\big) s_1^{-6} s_2^{-6} dn\, d^{\times}s\, d^{\times}\lambda dk. \qquad (13)$$

As every element of G_0 was assumed to have determinant greater than 1, the set $B(n, s_1, s_2, \lambda, X)$

is empty if $\lambda > X^{1/36}$. The integral of the error term in the integrand of (13) is computed to be

$$O\Big(\int_{\lambda=0}^{X^{1/36}} \int_{s_1,s_2=c}^{C\lambda/c^3} \lambda^{27} s_1^6 s_2^3 s_1^{-6} s_2^{-6} d^\times s\, d^\times \lambda\Big) = O(X^{3/4+\epsilon}).$$

Meanwhile, the integral of the main term in the integrand of (13) is equal to

$$\frac{1}{C_{G_0}} \int_{h\in G_0} \mathrm{Vol}(\mathcal{R}_X(L^\pm, h))dh - \Big(\int_{\lambda=0}^{X^{1/36}} \int_{s_1,s_2=C\lambda/c^3}^{\infty} \mathrm{Vol}(B(1,1,\lambda,X)) s_1^{-6} s_2^{-6} d^\times s\, d^\times \lambda\Big).$$

Since $\mathrm{Vol}(\mathcal{R}_X(L^\pm, h))$ is independent of h and $\mathrm{Vol}(B(1,1,\lambda,X)) = O(\lambda^{30})$, Equation (13) then implies that

$$N(V_{\mathbb{Z}}^\pm; X) = \frac{1}{3}\mathrm{Vol}(\mathcal{R}_X(L^\pm)) + o(X^{5/6}), \tag{14}$$

where $\mathcal{R}_X(L^\pm) := \mathcal{R}_X(L^\pm, 1)$.

Thus to prove Theorem 11, it remains only to compute the volume $\mathrm{Vol}(\mathcal{R}_X(L^\pm))$.

2.3 Computing the volume

Let $R_V^\pm := \Lambda L^\pm$ and let $R_V^\pm(X)$ denote the set of those points in $R_V^\pm$ having height less than X. Then since $\mathcal{F} = \mathcal{F}_{\mathrm{SL}_3}\Lambda$, where $\mathcal{F}_{\mathrm{SL}_3} \subset \mathrm{SL}_3(\mathbb{R})$ is a fundamental domain for the left action of $\mathrm{SL}_3(\mathbb{Z})$ on $\mathrm{SL}_3(\mathbb{R})$, we have $\mathcal{R}_X(L^\pm) = \mathcal{F}_{\mathrm{SL}_3} R_V^\pm$.

For each $(I, J) \in \mathbb{R}\times\mathbb{R}$ with $4I^3 - J^2 > 0$ (resp. $4I^3 - J^2 < 0$), the set R_V^+ (resp. R_V^-) contains exactly one point $p_{I,J}$ having invariants I and J. There is thus a natural measure dr on both the sets $R_V^\pm$, given by $dr = dIdJ$. Now define the usual subgroups $\bar{N}$, A, and N, of $\mathrm{SL}_3(\mathbb{R})$ as follows:

$$\begin{aligned}
\bar{N} &= \{\bar{n}(x) : x \in \mathbb{R}^3\}, \text{ where } \bar{n}(x) = \begin{pmatrix} 1 & x_1 & x_2 \\ & 1 & x_3 \\ & & 1 \end{pmatrix}; \\
A &= \{a(t) : t \in \mathbb{R}_+^{\times 2}\}, \text{ where } a(t) = \begin{pmatrix} t_1 & & \\ & t_2 & \\ & & t_1^{-1}t_2^{-1} \end{pmatrix}; \\
N &= \{n(u) : u \in \mathbb{R}^3\}, \text{ where } n(u) = \begin{pmatrix} 1 & & \\ u_1 & 1 & \\ u_2 & u_3 & 1 \end{pmatrix}.
\end{aligned}$$

It is well-known that the natural product map $\bar{N}\times A\times N \to H_{\mathbb{R}}$ maps injectively on to a full measure set in $\mathrm{SL}_3(\mathbb{R})$ and that this decomposition gives a Haar measure dg on $\mathrm{SL}_3(\mathbb{R})$ defined by $dg = t_1^{-4}t_2^{-2}dxdud^\times t_1 d^\times t_2$.

We have the following proposition:

Proposition 17 *For any measurable function ϕ on $V_{\mathbb{R}}$, we have*

$$\frac{1}{3}\cdot\frac{4}{3}\int_{R_V^\pm}\int_{\mathrm{SL}_2(\mathbb{R})} \phi(g\cdot p_{I,J}))\, dg\, dIdJ = \int_{V_{\mathbb{R}}^\pm} \phi(v)dv. \tag{15}$$

By Lemma 12, we see that $\mathrm{SL}_3(\mathbb{R})R_V^{\pm}$ is a 3-fold cover of a full measure set of $V_{\mathbb{R}}^{\pm}$; the proposition can then be verified by a Jacobian computation. However, we present a more general proof of Proposition 17 that does not depend on the specific form of the sets $R_V^{\pm}$. Specifically, we prove the following proposition which will also be useful to us in the sequel.

Proposition 18 *Let dg be the Haar measure on $\mathrm{SL}_3(\mathbb{C})$ obtained from the $\bar{N}AN$ decomposition. Let dv be the Euclidean measure on $V_{\mathbb{C}}$, the $\mathbb{C}$-vector space of all ternary cubic forms with complex coefficients. Let R be any subset of $V_{\mathbb{C}}$ that for each pair $(I,J) \in \mathbb{C} \times \mathbb{C}$ contains exactly one point $p_{I,J}$ having invariants equal to I and J, and such that G_0R is measurable for any measurable set $G_0 \subset \mathrm{SL}_3(\mathbb{C})$. Then for any measurable function ϕ on $V_{\mathbb{C}}$, we have*

$$\frac{1}{27} \cdot \frac{4}{3} \int_R \int_{\mathrm{SL}_2(\mathbb{C})} \phi(g \cdot p_{I,J})\, dg\, dI dJ = \int_{v \in V_{\mathbb{C}}} \phi(v) dv.$$

Proof: Analagously to Lemma 12, we have the following lemma whose proof we again defer to Section 3:

Lemma 19 *Let $f \in V_{\mathbb{C}}$ be any ternary cubic form having nonzero discriminant. Then the size of the stabilizer in $\mathrm{SL}_3(\mathbb{C})$ of f is equal to 27.*

It follows from Lemma 19 that $\mathrm{SL}_2(\mathbb{C}) \cdot R$ is a 27-fold cover of a full measure set in $V_{\mathbb{C}}$. For $(I,J) \in \mathbb{C} \times \mathbb{C}$, let $q_{I,J}(x,y)$ denote the special "Weierstrass" ternary cubic form $x^3 - \frac{I}{3}xz^2 - \frac{J}{27}z^3 - y^2z$ having invariants I and J. We first consider the single case $R = R_0$, where R_0 is defined by $R_0 := \{q_{I,J} : (I,J) \in \mathbb{C} \times \mathbb{C}\}$. In this case, the result follows from a Jacobian computation.

In the general case, we observe that if $p_{I,J} \in V_{\mathbb{C}}$ has invariants I and J with $4I^3 - J^2 \neq 0$, then $p_{I,J}$ has flexes defined over $\mathbb{C}$, and so by a change-of-variable can be expressed in Weierstrass normal form. In particular, there exists $g_{I,J} \in \mathrm{SL}_3(\mathbb{C})$ such that $g_{I,J} \cdot p_{I,J} = q_{I,J}$.

We now have

$$\begin{aligned} \int_{v \in \mathrm{SL}_3(\mathbb{C}) \cdot R} \phi(v) dv &= \frac{4}{3} \int_{R_0} \int_{\mathrm{SL}_2(\mathbb{C})} \phi(g \cdot q_{I,J}) dg dr = \frac{4}{3} \int_R \int_{\mathrm{SL}_2(\mathbb{C})} \phi(g g_{I,J} \cdot p_{I,J}) dg dr \\ &= \frac{4}{3} \int_R \int_{\mathrm{SL}_2(\mathbb{C})} \phi(g \cdot p_{I,J}) dg dr, \end{aligned}$$

where the last equality follows from the fact that $\mathrm{SL}_3(\mathbb{C})$ is a *unimodular* group (see [25, Chapter 8]), i.e., the left Haar measure dg is also a right Haar measure on $\mathrm{SL}_3(\mathbb{C})$. $\square$

Proposition 17 now follows from Proposition 18 and the principle of permanence of identities. We may use it to compute the volume of $\mathcal{R}_X(L^{\pm}) = \mathcal{F}_{\mathrm{SL}_3} R_V^{\pm}$ as follows. We have

$$\int_{\mathcal{R}_X(L^{\pm})} dv = \int_{\mathcal{F}_{\mathrm{SL}_3} R_V^{\pm}(X)} dv = \frac{4}{3} \int_{R_V^{\pm}(X)} \int_{\mathcal{F}_{\mathrm{SL}_3}} dg\, dI\, dJ = \frac{4\zeta(2)\zeta(3)}{3} \int_{R_V^{\pm}(X)} dI\, dJ. \tag{16}$$

The quantity $\int_{R_V^{+}(X)} dI\, dJ$ is equal to

$$\int_{I=0}^{X^{1/3}} \int_{J=-2I^{3/2}}^{2I^{3/2}} dI dJ = \int_{I=0}^{X^{1/3}} 4I^{3/2} dI = \frac{8}{5} I^{5/2}|_0^{X^{1/3}} = \frac{8}{5} X^{5/6}, \tag{17}$$

while $\int_{R_V^-(X)} dI\,dJ$ is equal to

$$\int_{I=-X^{1/3}}^{X^{1/3}} \int_{J=-2X^{1/2}}^{2X^{1/2}} dIdJ - \int_{R_V^+(X)} dIdJ = 8X^{5/6} - \frac{8}{5}X^{5/6} = \frac{32}{5}X^{5/6}. \tag{18}$$

We conclude that

$$\begin{aligned} \mathrm{Vol}(\mathcal{R}_X(L^+)) &= \frac{32\zeta(2)\zeta(3)}{15}X^{5/6}, \\ \mathrm{Vol}(\mathcal{R}_X(L^-)) &= \frac{128\zeta(2)\zeta(3)}{15}X^{5/6}, \end{aligned} \tag{19}$$

which along with (14) now yields Theorem 11.

2.4 Congruence conditions

In this subsection, we prove a version of Theorem 11 where we count integral ternary cubic forms satisfying any finite set of congruence conditions.

Suppose S is a subset of $V_{\mathbb{Z}}^{\pm}$ defined by finitely many congruence conditions. We may assume that $S \subset V_{\mathbb{Z}}^{\pm}$ is defined by congruence conditions modulo some integer m. Then S may be viewed as the intersection of $V_{\mathbb{Z}}^{\pm}$ with the union of k translates $\mathcal{L}_1, \ldots, \mathcal{L}_k$ of the lattice $m \cdot V_{\mathbb{Z}}$. For each such lattice translate $\mathcal{L}_j$, we may use formula (8) and the discussion following that formula to compute $N(\mathcal{L}_j \cap V_{\mathbb{Z}}^{\pm}; X)$, where each d-dimensional volume is scaled by a factor of $1/m^d$ to reflect the fact that our new lattice has been scaled by a factor of m. With these scalings, the maximum volume of the projections of $B(n, s_1, s_2, \lambda, X)$, is again seen to be at most $O(\lambda^{24} s_1^6 s_2^3)$. And once more, identically as in (14), we see that

$$N(\mathcal{L}_j \cap V_{\mathbb{Z}}^{\pm}; X) = \frac{\mathrm{Vol}(\mathcal{R}_X(L^{\pm}))}{3m^{10}} + o(X^{5/6}).$$

Summing over j, we thus obtain

$$N(S \cap V_{\mathbb{Z}}^{\pm}; X) = \frac{k\mathrm{Vol}(\mathcal{R}_X(L^{\pm}))}{3m^{10}} + o(X^{5/6}). \tag{20}$$

For any set S in $V_{\mathbb{Z}}$ that is definable by congruence conditions, let us denote by $\mu_p(S)$ the p-adic density of the p-adic closure of S in $V_{\mathbb{Z}_p}$, where we normalize the additive measure μ_p on $V_{\mathbb{Z}_p}$ so that $\mu_p(V_{\mathbb{Z}_p}) = 1$. We then have the following theorem:

Theorem 20 *Suppose S is a subset of $V_{\mathbb{Z}}^{\pm}$ defined by finitely many congruence conditions. Then we have*

$$N(S \cap V_{\mathbb{Z}}^{\pm}; X) = N(V_{\mathbb{Z}}^{\pm}; X) \prod_p \mu_p(S) + o(X^{5/6}), \tag{21}$$

where $\mu_p(S)$ denotes the p-adic density of S in $V_{\mathbb{Z}}$, and where the implied constant in $o(X^{5/6})$ depends only on S.

Theorem 20 follows from (20) and the discussion preceding it, coupled with the identity $km^{-10} = \prod_p \mu_p(S)$.

2.5 The number of reducible points in the main bodies of the fundamental domains is negligible (Proof of Lemma 15)

We may write $V_{\mathbb{Z}}^{\mathrm{red}} = V_{\mathbb{Z}}^{\mathrm{red},(1)} \cup V_{\mathbb{Z}}^{\mathrm{red},(2)}$, where $V_{\mathbb{Z}}^{\mathrm{red},(1)}$ denotes the set of all integral ternary cubic forms that have a rational flex in $\mathbb{P}^2$, and $V_{\mathbb{Z}}^{\mathrm{red},(2)}$ denotes the set of all integral ternary cubic forms in $V_{\mathbb{Z}} \setminus V_{\mathbb{Z}}^{\mathrm{red},(1)}$ whose Jacobian has at least one nontrivial 3-torsion point; in other words, $V_{\mathbb{Z}}^{\mathrm{red},(2)}$ consists of all points in $V_{\mathbb{Z}}$ that are strongly irreducible but not totally irreducible. We estimate

$$\int_{na(s_1,s_2)\lambda k \in \mathcal{F}'} \#\{x \in V_{\mathbb{Z}}^{\mathrm{red},(i)} \cap B(n,s_1,s_2,\lambda,X)\} s_1^{-6} s_2^{-6} dn\, d^\times t\, d^\times \lambda\, dk$$

separately for $i = 1$ and 2 in the following two lemmas.

Lemma 21 *Let $\mathcal{F}'$ denote the set of elements $na(s_1,s_2)\lambda k \in \mathcal{F}$ that satisfy $s_1 < 3C\lambda/c^3$ and $s_2 < 3C\lambda/c^3$. Then*

$$\int_{na(s_1,s_2)\lambda k \in \mathcal{F}'} \#\{x \in V_{\mathbb{Z}}^{\mathrm{red},(1)} \cap B(n,s_1,s_2,\lambda,X)\} s_1^{-6} s_2^{-6} dn\, d^\times t\, d^\times \lambda dk = o(X^{5/6}).$$

Proof: Suppose f is an integral ternary cubic form. If f has a rational flex in $\mathbb{P}^2$, then for all but finitely many primes p, the reduction $\bar{f}$ of f modulo p has a point of inflection in $\mathbb{P}^2(\mathbb{F}_p)$. Now let p be a sufficiently large prime that is congruent to 1 (mod 3), and let a, b, c be elements in $\mathbb{F}_p^\times$ that are in different cube classes (i.e., none of a/b, b/c, c/a are cubes in $\mathbb{F}_p^\times$). Then it may be checked that the ternary cubic form $f_{a,b,c}(x,y,z) = ax^3 + by^3 + cz^3 \in V_{\mathbb{F}_p}$ has no point of inflection in $\mathbb{F}_p$. Hence none of the forms in the set $S_p = \{\gamma \cdot f_{a,b,c} : \gamma \in \mathrm{GL}_3(\mathbb{F}_p)\}$ contain points of inflection in $\mathbb{F}_p$. It is clear that $\#S_p \gg p^9$, where the implied constant is independent of p. Thus, if s_p denotes the p-adic density of the set $V_{\mathbb{Z}}^{(1)}(p)$ of elements in $V_{\mathbb{Z}}$ whose reduction modulo p is contained in S_p, then $s_p \gg p^9/p^{10} = 1/p$, where the implied constant is independent of p. Since elements in $V_{\mathbb{Z}}^{(1)}(p)$ do not belong to $V_{\mathbb{Z}}^{\mathrm{red},(1)}$, we see that

$$\int_{na(s_1,s_2)\lambda k \in \mathcal{F}'} \#\{x \in V_{\mathbb{Z}}^{\mathrm{red},(1)} \cap B(n,s_1,s_2,\lambda,X)\} s_1^{-6} s_2^{-6} dn\, d^\times t\, d^\times \lambda dk \ll X^{5/6} \prod_{p \equiv 1\,(3)} (1 - s_p). \quad (22)$$

But since $s_p \gg 1/p$ independent of p, it follows that $\prod_{p\equiv 1\,(3)}(1-s_p)$ diverges, and hence the left hand side of (22) is $o(X^{5/6})$ as required. □

We now bound the number of $\mathrm{SL}_3(\mathbb{Z})$-equivalence classes of integral ternary cubic forms having bounded height that are strongly irreducible but not totally irreducible, i.e., those integral ternary cubic forms whose associated cubic curves have no rational flex in $\mathbb{P}^2$, but whose Jacobians contain a nontrivial 3-torsion point.

Lemma 22 *The number of $\mathrm{SL}_3(\mathbb{Z})$-equivalence classes of integral ternary cubic forms that are strongly irreducible but not totally irreducible having height bounded by X is $o(X^{5/6})$.*

Proof: By Equation (12) and Lemma 14, it suffices to prove the estimate

$$\int_{na(s_1,s_2)\lambda k \in \mathcal{F}'} \#\{x \in V_{\mathbb{Z}}^{\mathrm{red},(2)} \cap B(n,s_1,s_2,\lambda,X)\} s_1^{-6} s_2^{-6} dn\, d^\times t\, d^\times \lambda dk = o(X^{5/6}). \quad (23)$$

The Jacobian of a form $f \in V_{\mathbb{Z}}$ may be embedded in $\mathbb{P}^2$ as a Weierstrass elliptic curve $\mathrm{Jac}(f)$ via the equation

$$y^2z = x^3 - \frac{I}{3}xz^2 - \frac{J}{27}z^3,$$

and under this embedding, the 3-torsion points of the Jacobian of f are precisely the flex points in $\mathbb{P}^2$ of the curve $\mathrm{Jac}(f)$. Thus an integral ternary cubic form f is contained in $V_{\mathbb{Z}}^{\mathrm{red},(2)}$ if and only if the curve $\mathrm{Jac}(f)$ contains at least 2 rational flex points in $\mathbb{P}^2$. The proof of the estimate in (23) now proceeds very similarly to that of Lemma 21. The only difference is that we now consider, for each $p \equiv 7 \pmod{12}$, the form $f_b(x,y,z) = x^3 + bz^3 - y^2z \in V_{\mathbb{F}_p}$, where b is a nonresidue in $\mathbb{F}_p$. We see that $\mathrm{Jac}(f)$ is precisely the curve defined by the equation $f = 0$, and it has exactly one inflection point in $\mathbb{P}^2(\mathbb{F}_p)$, namely the point $[0:1:0]$. $\square$

Lemma 15 now follows from Lemmas 21 and 22.

2.6 The average number of strongly irreducible integral ternary cubic forms with given invariants (Proofs of Theorems 9 and 10)

We first prove Theorem 9, by describing the set of *eligible* pairs $(I,J) \in \frac{1}{16}\mathbb{Z} \times \frac{1}{32}\mathbb{Z}$, i.e., those pairs that occur as invariants of integral ternary cubic forms. We begin by showing that a pair (I,J) is eligible if and only if it occurs as the invariants of a Weierstrass elliptic curve over $\mathbb{Z}$:

Proposition 23 *A pair (I,J) is eligible if and only if it occurs as the invariants of some Weierstrass cubic over $\mathbb{Z}$, where a Weierstrass cubic over $\mathbb{Z}$ is an element in $V_{\mathbb{Z}}$ of the form*

$$y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3.$$

Proof: This theorem is easily deduced from the results in [2]. To any integral ternary cubic form $f \in V_{\mathbb{Z}}$, one may associate a Weierstrass ternary cubic form f^* over $\mathbb{Z}$ which defines the Jacobian curve (see [2, Equation 1.5]). The invariants $c_4(f)$ and $c_6(f)$ of f are then defined to be equal to the classical invariants $c_4(f^*)$ and $c_6(f^*)$ of the corresponding Weierstrass cubic (see [29] for a definition of $c_4(f^*)$ and $c_6(f^*)$). Using [2, Equation 1.7], we easily check that our invariants I and J are equal to the invariants $c_4/16$ and $c_6/32$, respectively, for any ternary cubic form. We thus conclude that $I(f) = I(f^*)$ and $J(f) = J(f^*)$, and the theorem follows. $\square$

Next, we have a result of Kraus (see [26, Proposition 2]) which describes those pairs (c_4, c_6) that can occur for a Weierstrass cubic over $\mathbb{Z}$:

Proposition 24 *Let c_4 and c_6 be integers. In order for there to exist a Weierstrass cubic over $\mathbb{Z}$ having nonzero discriminant and invariants c_4 and c_6, it is necessary and sufficient that*

(a) $(c_4^3 - c_6^2)/1728$ *is a nonzero integer*;

(b) $c_6 \not\equiv \pm 9 \pmod{27}$;

(c) *either* $c_6 \equiv -1 \pmod 4$, *or* $c_4 \equiv 0 \pmod{16}$ *and* $c_6 \equiv 0, 8 \pmod{32}$.

It can be checked that the set of pairs (I,J) that satisfy the congruence conditions of Theorem 9 is the same as the set of pairs $(c_4/16, c_6/32)$ for which the congruence conditions of Proposition 24 are satisfied for (c_4, c_6). Thus Theorem 9 follows from Propositions 23, 24, and the fact that $I(f) = c_4(f)/16$ and $J(f) = c_6(f)/32$ for Weierstrass cubics f having integral coefficients.

We now use Theorem 9 to count the number of eligible pairs $(I,J) \in \frac{1}{16}\mathbb{Z} \times \frac{1}{32}\mathbb{Z}$ having bounded height:

Proposition 25 *Let $N^+_{I,J}(X)$ and $N^-_{I,J}(X)$ denote the number of eligible pairs $(I,J) \in \frac{1}{16}\mathbb{Z} \times \frac{1}{32}\mathbb{Z}$, satisfying $H(I,J) < X$, that have positive discriminant and negative discriminant, respectively. Then*

(a) $N^+_{I,J}(X) = \dfrac{32}{135}X^{5/6} + O(X^{1/2})$;

(a) $N^-_{I,J}(X) = \dfrac{128}{135}X^{5/6} + O(X^{1/2})$.

Proof: Let $R^+(X)$ (resp. $R^-(X)$) denote the set of points $(p_1,p_2) \in \mathbb{R}\times\mathbb{R}$ satisfying $H(p_1,p_2) < X$ and $4p_1^3 - p_2^2 > 0$ (resp. $4p_1^3 - p_2^2 < 0$). Then an easy application of Proposition 16 gives

$$N^\pm_{I,J}(X) = \frac{16\cdot 32}{128\cdot 27}\mathrm{Vol}(R^\pm(X)) + O(X^{1/2}).$$

Now the volumes of the sets $R^+(X)$ and $R^-(X)$ have been computed in Equations (17) and (18) to be equal to $8/5$ and $32/5$, respectively, and the proposition follows. □

Theorem 8 combined with Proposition 25 now yields Theorem 10.

3 The average number of elements in the 3-Selmer group of elliptic curves

Recall that any isomorphism class of elliptic curve E over $\mathbb{Q}$ has a unique representative of the form

$$E(A,B) : y^2 = x^3 + Ax + B, \tag{24}$$

where $A, B \in \mathbb{Z}$ and $p^4 \nmid A$ if $p^6 \mid B$. For any elliptic curve $E(A,B)$ over $\mathbb{Q}$ written in the form (24), we define the quantities $I(E)$ and $J(E)$ by

$$I(E) = -3A, \tag{25}$$

$$J(E) = -27B. \tag{26}$$

We then define the *height* $H(E)$ of E by

$$H(E) := \max(|I(E)|^3, J(E)^2/4).$$

In this section, we prove Theorem 3 by bounding the average size of the 3-Selmer group of rational elliptic curves, when these curves are ordered by their heights. In fact, we prove a stronger version of this theorem. To state this stronger version, we need some notation. If F is a family of elliptic curves defined by local conditions, then let F^{inv} denote the set $\{(I(E),J(E)) : E \in F\}$. For a prime p, let F^{inv}_p denote the p-adic closure of F^{inv} in $\mathbb{Z}_p \times \mathbb{Z}_p$ and let F_p denote the space of all elliptic curves over $\mathbb{Q}_p$ that have invariants $(I,J) \in F^{\mathrm{inv}}_p$. We then say that F is *acceptable at* p if F_p contains at least all those elliptic curves over $\mathbb{Q}_p$ whose discriminants are not divisible by p^2. We say that F is *acceptable* if F is acceptable at p for all sufficiently large primes p. Then, in this section, we prove the following theorem.

Theorem 26 *When elliptic curves E in any acceptable family are ordered by height, the average size of the 3-Selmer group $S_3(E)$ is bounded above by 4.*

It is clear that the set of all elliptic curves is acceptable. So too is the set of all elliptic curves satisfying a finite set of prescribed local conditions. Note also that the set of semistable elliptic curves is acceptable because if E is an elliptic curve over $\mathbb{Q}$ that has additive reduction over a prime p, then p^2 divides the discriminant of E.

Remark on notation Unlike the introduction, we denote the elliptic curve $E : y^2 = x^3 + Ax + B$ by $E(A, B)$ in this section. Also, from hereon in, we denote the elliptic curve having invariants equal to I and J by $E_{I,J}$.

3.1 Integral ternary cubic forms and the 3-Selmer group of elliptic curves

An element $\mathcal{C}$ in the 3-Selmer group of an elliptic curve $E/\mathbb{Q}$ may be thought of as a locally soluble 3-covering of $E/\mathbb{Q}$. It then follows from a result of Cassels [12, Theorem 1.3] that $\mathcal{C}$ has a degree 3 divisor defined over $\mathbb{Q}$ yielding an embedding of $\mathcal{C}$ into $\mathbb{P}^2$ defined over $\mathbb{Q}$, and therefore a ternary cubic form f with rational coefficients. As $\mathcal{C}$ is locally soluble, this ternary cubic form f will be *locally soluble*, i.e, the curve $f(x, y, z) = 0$ has points in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all primes p.

Conversely, every locally soluble ternary cubic form over $\mathbb{Q}$, having invariants I and J, defines a 3-covering over its Jacobian $E : y^2 = x^3 - \frac{I}{3}x - \frac{J}{27}$. The explicit map from the cubic curve $\mathcal{C}$ defined by $f = 0$ to E may be described in terms of the various SL_3-covariants of f. A ternary cubic form f has six fundamental covariants. Apart from f itself, the invariants $I(f)$ and $J(f)$ of f, and the Hessian $\mathcal{H}(f)$ of f, we have in addition the *bordered Hessian* $\mathcal{G}(f)$ of f and the Jacobian $\mathcal{J}$ of f, $\mathcal{H}$, and $\mathcal{G}$ defined by:

$$\mathcal{G}(f(x,y,z)) := \begin{vmatrix} f_{xx} & f_{xy} & f_{xz} & \mathcal{H}_x \\ f_{xy} & f_{yy} & f_{yz} & \mathcal{H}_y \\ f_{xz} & f_{yz} & f_{zz} & \mathcal{H}_z \\ \mathcal{H}_x & \mathcal{H}_y & \mathcal{H}_z & 0 \end{vmatrix}; \quad \mathcal{J}(f(x,y,z)) := \begin{vmatrix} f_x & \mathcal{H}_x & \mathcal{G}_x \\ f_y & \mathcal{H}_y & \mathcal{G}_y \\ f_z & \mathcal{H}_z & \mathcal{G}_z \end{vmatrix}. \tag{27}$$

(see, e.g., [18] for a discussion and proof). The covariants $f(X, Y, Z)$, $\mathcal{H}(X, Y, Z)$, $\mathcal{G}(X, Y, Z)$, and $\mathcal{J}(X, Y, Z)$ are covariants of degrees 1, 3, 8, and 12, respectively, in the coefficients of f and of degrees 3, 3, 6, and 9, respectively, in X, Y, and Z. The explicit map ψ_f from $\mathcal{C}$ to E is then given in [1, Equation 13] to be

$$\psi_f : [X, Y, Z] \mapsto \left(\frac{\mathcal{G}(X, Y, Z)}{\mathcal{H}(X, Y, Z)^2}, \frac{\mathcal{J}(X, Y, Z)}{9\mathcal{H}(X, Y, Z)^3} \right). \tag{28}$$

Now two ternary cubic forms $f, g \in V_{\mathbb{Q}}$ cut out the same cubic curves in $\mathbb{P}^2$, up to an automorphism of $\mathbb{P}^2$ over $\mathbb{Q}$, if and only if f and g are equivalent under the action $\mathbb{G}_m \times \mathrm{GL}_3(\mathbb{Q})$, where $\mathbb{G}_m(\mathbb{Q}) = \mathbb{Q}^\times$ acts on $V_{\mathbb{Q}}$ by scalar multiplication; we then say simply that f and g are *equivalent*. However, equivalent forms f, g having the same invariants I, J do not necessarily give the same 3-covering mapping in (28). Indeed, if $g = \gamma \cdot f$, where $\gamma = (\gamma_1, \gamma_2) \in \mathbb{G}_m \times \mathrm{GL}_3(\mathbb{Q})$, then for g and f to have the same invariants we must have $\det(\gamma) := \gamma_1 \det(\gamma_2) = \pm 1$, since $I(g) = \det(\gamma)^4 I(f)$ and $J(g) = \det(\gamma)^6 J(f)$. Now since $\mathcal{H}(f)$ has odd degree in the coefficients of f, while $\mathcal{G}(f)$ and $\mathcal{J}(f)$ each have even degree, all (28) implies is that

$$\psi_g([X, Y, Z]) = \psi_{\gamma \cdot f}([X, Y, Z]) = \gamma_1 \det(\gamma_2) \cdot \psi_f([X, Y, Z] \cdot \gamma_2) = \pm \psi_f([X, Y, Z] \cdot \gamma_2), \tag{29}$$

where $-\psi_f([X, Y, Z] \cdot \gamma_2)$ refers to the negative of $\psi_f([X, Y, Z] \cdot \gamma_2)$ considered as a point on the elliptic curve E. That is, equivalent ternary cubic forms f and g that have the same invariants

will always yield 3-coverings that are either the same or are inverse elements in the Weil-Chatelet group (or in the 3-Selmer group, if they are locally soluble). In particular, note that the ternary cubic forms f and $-f$ yield 3-coverings that are inverse to each other.

Hence, in order to exactly parametrize elements in the 3-Selmer groups of elliptic curves—and not collapse 3-Selmer elements with their inverses—it is natural to consider a notion of *proper equivalence* on ternary cubic forms, where we now allow equivalence only by those elements $(\gamma_1, \gamma_2) \in \mathbb{G}_m \times \mathrm{GL}_3(\mathbb{Q})$ for which $\gamma_1 \det(\gamma_2) = 1$. In particular, the forms f and $-f$ are then not properly equivalent unless f contains a rational flex point. The 3-coverings of an elliptic curve $E = E_{I,J}$ are then exactly parametrized by proper equivalence classes of forms $f \in V_{\mathbb{Q}}$ having invariants I, J.

Alternatively, consider the action of $\mathrm{PGL}_3(\mathbb{Q})$ on $V_{\mathbb{Q}}$ defined by

$$(\gamma \cdot f)(x, y, z) = (\det\ \gamma)^{-1} f((x, y, z) \cdot \gamma),$$

where $\gamma \in \mathrm{GL}_3(\mathbb{Q})$ and $f \in V_{\mathbb{Q}}$. Since it is clear that the center of $\mathrm{GL}_3(\mathbb{Q})$ acts trivially, we obtain a well-defined action of $\mathrm{PGL}_3(\mathbb{Q})$ on $V_{\mathbb{Q}}$. (In the identical manner, if R is any ring, then we also obtain a well-defined action of $\mathrm{PGL}_3(R)$ on V_R.) It is also then clear that two ternary cubic forms $f, g \in V_{\mathbb{Q}}$ are properly equivalent if and only if they are $\mathrm{PGL}_3(\mathbb{Q})$-equivalent. We thus have the following proposition.

Proposition 27 *Let $E/\mathbb{Q}$ be an elliptic curve. Then the elements in the 3-Selmer group of E are in bijective correspondence with $\mathrm{PGL}_3(\mathbb{Q})$-orbits on the set of locally soluble ternary cubic forms in $V_{\mathbb{Q}}$ having invariants equal to $I(E)$ and $J(E)$.*

By [13, Theorem 1.1], any rational ternary cubic form $f \in V_{\mathbb{Q}}$ having integral invariants I and J is equivalent to an integral ternary cubic form $g \in V_{\mathbb{Z}}$ having invariants I and J. In particular, it follows that such an f is properly equivalent to either g or $-g$. Since g and $-g$ have the same invariants, we obtain the following proposition:

Proposition 28 *Let $E/\mathbb{Q}$ be an elliptic curve. Then the elements in the 3-Selmer group of E are in bijective correspondence with $\mathrm{PGL}_3(\mathbb{Q})$-orbits on the set of locally soluble integral ternary cubic forms in $V_{\mathbb{Z}}$ having invariants equal to $I(E)$ and $J(E)$.*

Next, recall that if K is any field and E is an elliptic curve defined over K, then equivalence classes of soluble 3-coverings of E over K correspond bijectively to elements in $E(K)/3E(K)$. These 3-coverings of E over K correspond to K-soluble ternary cubic forms over K, where a ternary cubic form f having coefficients in K is said to be *K-soluble* if the equation $f(x, y, z) = 0$ has a solution with $[x : y : z] \in \mathbb{P}^2(K)$.

We thus have the following lemma which will be necessary for us later on.

Lemma 29 *Let K be a field and E be any elliptic curve over K. Then there exists a natural injection*

$$\mathcal{T}_E : E(K)/3E(K) \to \{\mathrm{PGL}_3(K)\text{-equivalence classes of ternary cubic forms over } K\},$$

whose image consists exactly of the K-soluble ternary cubic forms having invariants equal to $I(E)$ and $J(E)$.

Finally, a 3-covering $\mathcal{C}$ of an elliptic curve E/K can be considered as a principal homogeneous space for E/K. The curves E and $\mathcal{C}$ are isomorphic over $\overline{K}$ and the automorphisms of $\mathcal{C}$ over $\overline{K}$ correspond to the 3-torsion points of $E(\overline{K})$. In fact, a 3-torsion point of $E(\overline{K})$ yields an automorphism of $\mathcal{C}$ simply via the action of E on C. Furthermore, this automorphism is defined over K if and only if the 3-torsion point in question is itself defined over K. We thus obtain:

Lemma 30 *Suppose E is an elliptic curve over a field K and f is a ternary cubic form over K having invariants equal to $I(E)$ and $J(E)$. Then the size of the stabilizer of f in $\mathrm{PGL}_3(K)$ is equal to $\#E(K)[3]$, the number of 3-torsion elements of E defined over K.*

We may use Lemma 30 to prove Lemmas 12, 13, and 19:

Proof of Lemmas 12 and 19: Let $f \in V_{\mathbb{R}}$ be a ternary cubic form having nonzero discriminant. By Lemma 30, if f has invariants I and J, then the size of the stabilizer of f in $\mathrm{PGL}_3(\mathbb{R})$ is equal to the number of real 3-torsion points on the elliptic curve $E/\mathbb{R}$ having invariants I and J. Now the 3-torsion points of a plane elliptic curve are its flex points, and it is known that any plane cubic curve over $\mathbb{R}$ having nonzero discriminant has exactly 3 flex points defined over $\mathbb{R}$ (see, e.g., [21, Chapter 13]). Now if $\gamma \in \mathrm{GL}_3^+(\mathbb{R})$ stabilizes f, then $I(\gamma \cdot f) = (\det \gamma)^4 I(f)$ and $J(\gamma \cdot f) = (\det \gamma)^6 J(f)$ and so $\det \gamma = 1$. Thus Lemma 12 follows.

Similarly, let $f \in V_{\mathbb{C}}$ be a ternary cubic form having nonzero discriminant. Then since every elliptic curve over $\mathbb{C}$ has nine 3-torsion points, we see that the stabilizer of f in $\mathrm{PGL}_3(\mathbb{C})$ (and therefore also $\mathrm{PSL}_3(\mathbb{C})$) has 9 elements. Lemma 19 now follows as there are exactly 3 elements in the center of $\mathrm{SL}_3(\mathbb{C})$ that stabilize f. □

Proof of Lemma 13: If a ternary cubic form $f \in V_{\mathbb{Z}}$ had nontrivial stabilizer in $\mathrm{SL}_3(\mathbb{Z})$, then its Jacobian would have a nontrivial 3-torsion point defined over $\mathbb{Q}$, contradicting the assumption that f is totally irreducible. □

Lemma 30 will also be extremely useful to us later on.

3.2 Computations of p-adic densities in terms of local masses

Proposition 27 asserts that elements in the 3-Selmer group of an elliptic curve over $\mathbb{Q}$, having invariants I and J, are in bijection with $\mathrm{PGL}_3(\mathbb{Q})$-orbits in the set of locally soluble integral ternary cubic forms having invariants I and J. For any pair $(I, J) \in \mathbb{Z} \times \mathbb{Z}$, let $C_1, \ldots, C_k$ be a set of $\mathrm{PGL}_3(\mathbb{Z})$-orbits on the set of integral ternary cubic forms having invariants equal to I and J. Let $C_{i_1}, \ldots, C_{i_\ell}$ be a maximal set of $\mathrm{PGL}_3(\mathbb{Q})$-inequivalent classes among the $C_1, \ldots, C_k$. We define $S^{I,J}$ to be the union of all the integral ternary cubic forms in C_{i_j}, where j ranges from 1 to ℓ. Then for a family F of elliptic curves, we define S^F to be union of $S^{I,J}$, where (I, J) range over elements in F^{inv}.

In this section we determine the p-adic density $\mu_p(S^F)$ of the set $S^F \subset V_{\mathbb{Z}}$ in terms of a *local* (*p-adic*) *mass* $M_p(V, F)$ of all isomorphism classes of soluble 3-coverings of elliptic curves over $\mathbb{Q}_p$; here the measure μ_p is normalized so that $\mu_p(V_{\mathbb{Z}}) = 1$.

Proposition 31 *We have $\mu_p(S^F) = |4/9|_p \cdot M_p(V, F)$, where*

$$M_p(V, F) = \Big(1 - \frac{1}{p^2}\Big)\Big(1 - \frac{1}{p^3}\Big) \int_{(I,J) \in F_p^{\mathrm{inv}}} \sum_{\sigma \in S_3(E_{I,J})} \frac{1}{\#E_{I,J}(\mathbb{Q}_p)[3]} dI dJ. \tag{30}$$

Proof: Let S_p^F denote the p-adic closure of S^F in $V_{\mathbb{Z}_p}$. For $(I, J) \in F_p^{\mathrm{inv}}$, let $B_p^{I,J}$ consist of a set of representatives $f_1, \ldots, f_k \in V_{\mathbb{Z}_p}$ for the action of $\mathrm{PGL}_3(\mathbb{Q}_p)$ on the set of soluble ternary cubic forms in $V_{\mathbb{Z}_p}$ having invariants equal to I and J. Define B_p^F by

$$B_p^F := \bigcup_{\substack{(I,J) \in F_p^{\mathrm{inv}} \\ f \in B_p^{I,J}}} \mathrm{PGL}_3(\mathbb{Z}_p) \cdot f.$$

The p-adic density $\mu_p(S_p^F)$ can be determined from the set B_p^F; namely, we have

$$\int_{v\in S_p^F} dv = \int_{f\in B_p^F} \frac{1}{\#\mathrm{Aut}(f)} df \ ,$$

where $\mathrm{Aut}(f)$ denotes the stabilizer of f in $\mathrm{PGL}_3(\mathbb{Q}_p)$. The latter integral can be computed using a Jacobian change of variables; indeed, Proposition 18 and the principle of permanence of identities imply that

$$\int_{f\in B_p^F} \frac{1}{\#\mathrm{Aut}(f)} df = |4/3|_p \mathrm{Vol}(\mathrm{PGL}_3(\mathbb{Z}_p)) \int_{(I,J)\in F_p^{\mathrm{inv}}} \sum_{f\in B_p^{I,J}} \frac{1}{\#\mathrm{Aut}(f)}.$$

By Lemmas 29 and 30, elements $f \in B_p^{I,J}$ correspond bijectively with elements $\sigma \in E_{I,J}(\mathbb{Q}_p)/3E_{I,J}(\mathbb{Q}_p)$, and the cardinality of $\mathrm{Aut}(f)$ is equal to the cardinality of $E_{I,J}(\mathbb{Q}_p)[3]$. Proposition 31 now follows because the volume of $\mathrm{PGL}_3(\mathbb{Z}_p)$ with respect to the Haar measure obtained from the $\bar{N}AN$ decomposition of $\mathrm{PGL}_3(\mathbb{Q}_p)$ is equal to $(1-1/p^2)(1-1/p^3)$ for $p \neq 3$ and to $3(1-1/3^2)(1-1/3^3)$ for $p=3$. $\square$

3.3 The number of elliptic curves of bounded height in an acceptable family

Suppose F is an acceptable family of elliptic curves. To prove Theorem 26 by bounding the average number of elements in the 3-Selmer groups of elliptic curves in F from above, we shall need to estimate the number of elliptic curves in F that have height bounded by X. In this section, we determine exact asymptotics for the number of elliptic curves having bounded height in any acceptable family F of elliptic curves.

As an elliptic curve is determined by its invariants I and J, we estimate the number of pairs (I,J) that belong to F^{inv} and have height less than X. It follows from an easy application of Proposition 16 that the number of pairs $(I,J) \in \mathbb{Z}\times\mathbb{Z}$ satisfying $H(I,J) < X$ and $4I^3 - J^2 > 0$ (resp. $H(I,J) < X$ and $4I^3 - J^2 < 0$) is equal to the volume of $R^+(X)$ (resp. $R^-(X)$) with an error of $O(X^{1/2})$.

Now, the set $F^{\mathrm{inv}} \subset \mathbb{Z}\times\mathbb{Z}$ is defined by (perhaps infinitely many) congruence conditions. Just as in [7, §5], define the local mass $M_p(U_1, F)$ by

$$M_p(U_1, F) = \int_{(I,J)\in F_p^{\mathrm{inv}}} dI dJ. \tag{31}$$

For any set $S \subset \mathbb{Z}\times\mathbb{Z}$, let $N(S^+;X)$ and $N(S^-;X)$ denote the number of pairs $(I,J) \in S$, having height bounded by X, satisfying $4I^3 - J^2 > 0$ and $4I^3 - J^2 < 0$, respectively. Then since $F^{\mathrm{inv}} = \cap_p (F_p^{\mathrm{inv}} \cap \mathbb{Z}\times\mathbb{Z})$, we have

$$\limsup_{X\to\infty} \frac{N(F^{\mathrm{inv},\pm};X)}{X^{5/6}} \leq \mathrm{Vol}(R^\pm) \prod_p M_p(U_1, F).$$

To prove a lower bound for $N(F^{\mathrm{inv},\pm};X)$, we need the following uniformity estimate:

Proposition 32 *The number of elliptic curves E over $\mathbb{Q}$ having height less than X such that p^2 divides the discriminant of E is $O(X^{5/6}/p^{4/3})$, where the implied constant is independent of p.*

Proof: If an elliptic curve $E/\mathbb{Q}$ has additive reduction at a prime p, then p^2 divides the discriminant of E. We start by bounding the number of elliptic curves that have additive reduction at p and height less than X. It can be checked that if an elliptic curve over $\mathbb{Q}$ having invariants I and J has additive reduction at a prime $p > 3$, then p divides both I and J. We now have the following lemma.

Lemma 33 *The number of integer pairs $(I, J) \neq (0, 0)$ having height less than X such that $p \mid I$ and $p \mid J$ is $O(X^{5/6}/p^{4/3})$, where the implied constant is independent of p.*

Proof: Let $N_p(X)$ be the number of pairs $(I, J) \in \mathbb{Z} \times \mathbb{Z}$ such that $H(I, J) < X$, $p \mid I$, and $p \mid J$. It follows from the definition of $N_p(X)$ that, independent of p, we have $N_p(X) = O(X^{5/6}/p^2 + X^{1/2}/p + 1)$. If $p \mid I$, $p \mid J$, for some pair $(I, J) \neq (0, 0)$ having height less than X, then we see that $p < 2X^{1/2}$ and so if $p > 2X^{1/2}$, then $N_p(X) = 0$. It then easily follows that $N_p(X) = O(X^{5/6}/p^{4/3})$, where the implied constant is independent of p. $\square$

To complete the proof of the proposition, it suffices to bound the number of pairs $(I, J) \in \mathbb{Z} \times \mathbb{Z}$ such that $H(I, J) < X$, the discriminant of the polynomial $f_{I,J} = x^3 - \frac{I}{3}x - \frac{J}{27}$ is divisible by p^2, and the reduction of $f_{I,J}$ modulo p does not have a triple root in $\mathbb{F}_p$. It can be checked that the latter two conditions are satisfied if and only if there exists an element $r \in \mathbb{Z}$ such that $r \pmod p$ is a double root of $f_{I,J} \pmod p$, and moreover $f_{I,J}(r)$ is divisible by p^2. Now [7, Proposition 3.17], which states that the number of such $f_{I,J}$ having height bounded by X is $O(X^{5/6}/p^{4/3})$ (where again the implied constant is independent of p), yields Proposition 32. $\square$

Let $\mathcal{A}_p$ denote the set of all elliptic curves whose discriminant is divisible by p^2. As F is acceptable, we have

$$\bigcap_{p \leq Y} (F_p^{\text{inv}} \cap \mathbb{Z} \times \mathbb{Z}) \subset F^{\text{inv}} \cup \bigcup_{p > Y} \mathcal{A}_p^{\text{inv}}$$

which in conjunction with Proposition 32 implies that

$$\liminf_{X \to \infty} \frac{N(F^{\text{inv},\pm}; X)}{X^{5/6}} \geq \text{Vol}(R^{\pm}) \prod_p M_p(U_1, F).$$

We therefore have the following theorem.

Theorem 34 *Let F be an acceptable family of elliptic curves and let $N(F; X)$ denote the number of elliptic curves in F that have height bounded by X. Then*

$$N(F; X) = (\text{Vol}(R^+) + \text{Vol}(R^-))X^{5/6} \prod_p M_p(U_1, F) + o(X^{5/6}). \tag{32}$$

3.4 Proof of the main theorem (Theorem 26)

Theorem 26 will be deduced from the following result:

Theorem 35 *Let F be an acceptable family of elliptic curves. Then*

$$\lim_{X \to \infty} \frac{\sum\limits_{\substack{E \in F \\ H(E) < X}} (\#S_3(E) - 1)}{\sum\limits_{\substack{E \in F \\ H(E) < X}} 1} \leq \zeta(2)\zeta(3) \prod_p \frac{M_p(V, F)}{M_p(U_1, F)}. \tag{33}$$

Proof: The numerator of the expression in the left hand side of (33) is equal to $N(S^F; X)$. Furthermore, identically as in Section 3.3, we see that

$$\begin{aligned} N(S^F; X) &\leq N(V_{\mathbb{Z}}; X) \prod_p \mu_p(S^F) \\ &= (N(V_{\mathbb{Z}}^+; X) + N(V_{\mathbb{Z}}^-; X)) \prod_p |4/9|_p M_p(V, F) \\ &= \frac{4}{9}\zeta(2)\zeta(3)(\mathrm{Vol}(R_X^+) + \mathrm{Vol}(R_X^-)) \prod_p |4/9|_p M_p(V, F) \\ &= \zeta(2)\zeta(3)(\mathrm{Vol}(R^+) + \mathrm{Vol}(R^-)) X^{5/6} \prod_p M_p(V, F). \end{aligned} \tag{34}$$

Taking the ratio of (34) and (32), we obtain the theorem. □

To evaluate the right hand side of (33) we need the following fact whose proof is identical to that of [11, Lemma 3.1]:

Lemma 36 *Let E be an elliptic curve over $\mathbb{Q}_p$. We have*

$$\#(E(\mathbb{Q}_p)/3E(\mathbb{Q}_p)) = \begin{cases} \#E[3](\mathbb{Q}_p) & \text{if } p \neq 3; \\ 3 \cdot \#E[3](\mathbb{Q}_p) & \text{if } p = 3; \end{cases}$$

Proof: A well-known result of Lutz (see, e.g., [29, Chapter 7, Proposition 6.3] for a proof) asserts that there exists a subgroup $M \subset E(\mathbb{Q}_p)$ of finite index that is isomorphic to $\mathbb{Z}_p$. Let G denote the finite group $E(\mathbb{Q}_p)/M$. Then by applying the snake lemma to the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & E(\mathbb{Q}_p) & \longrightarrow & G & \longrightarrow & 0 \\ \downarrow & & \downarrow{\scriptstyle [3]} & & \downarrow{\scriptstyle [3]} & & \downarrow{\scriptstyle [3]} & & \downarrow \\ 0 & \longrightarrow & M & \longrightarrow & E(\mathbb{Q}_p) & \longrightarrow & G & \longrightarrow & 0 \end{array}$$

we obtain the exact sequence

$$0 \to M[3] \to E(\mathbb{Q}_p)[3] \to G[3] \to M/3M \to E(\mathbb{Q}_p)/3E(\mathbb{Q}_p) \to G/3G \to 0.$$

Since G is a finite group and M is isomorphic to $\mathbb{Z}_p$, Lemma 36 follows. □

By Equations (30) and (31), the right hand side of (33) is equal to

$$\zeta(2)\zeta(3) \prod_p \left(1 - \frac{1}{p^2}\right)\left(1 - \frac{1}{p^3}\right) \frac{\displaystyle\prod_p \int_{(I,J) \in F_p^{\mathrm{inv}}} \sum_{\sigma \in E_{I,J}/3E_{I,J}} \frac{1}{\#E[3](\mathbb{Q}_p)} dI dJ}{\displaystyle\prod_p \int_{(I,J) \in F_p^{\mathrm{inv}}} dI dJ},$$

which is then equal to 3 by Lemma 36. We have proven Theorem 26, and thus also Theorems 1 and 3.

4 A positive proportion of elliptic curves have rank 0

We have shown in the previous section that the average rank of all elliptic curves, when ordered by height, is less than 1.17. This immediately implies that a large proportion (indeed, at least 62.5%) of all elliptic curves must have rank 0 *or* 1.

In order to deduce analogous positive proportion statements for the individual ranks 0 and 1, we may attempt to make use of information regarding the distribution of the *parity* of the ranks—or of the 3-Selmer ranks—of these curves. Indeed, if we knew that even and odd 3-Selmer ranks occur equally often in an acceptable family of elliptic curves, then this would imply by Theorem 26 that a positive proportion of curves in that family have rank 0, and (assuming finiteness of the Tate–Shafarevich group) a positive proportion have rank 1.

In Section 4.1 we will show, using a recent result of Dokchitser–Dokchitser [19], how to construct positive proportion, acceptable families F of elliptic curves in which the parities of the 3-Selmer ranks of the curves in F are equally distributed between even and odd, thus unconditionally yielding a positive proportion of elliptic curves having rank 0.

We may also combine our counting techiques with the recent work of Skinner–Urban [30], in order to deduce that a positive proportion of all elliptic curves, when ordered by height, have *analytic rank* 0; i.e., a positive proportion of all elliptic curves have non-vanishing L-function $\mathrm{L}(E,s)$ at $s=1$. Since these analytic rank 0 curves yield a subset of the rank 0 curves of Section 4.1, it follows that a positive proportion of all elliptic curves satisfy the Birch and Swinnerton-Dyer conjecture. This is discussed in Section 4.2.

4.1 Elliptic curves having algebraic rank 0

Recall that the conjecture of Birch and Swinnerton-Dyer implies, in particular, that the evenness or oddness of the rank of an elliptic curve E is determined by whether its *root number*—that is, the sign of the functional equation of the L-function $\mathrm{L}(E,s)$ of E—is $+1$ or -1, respectively. It is widely believed that the root numbers $+1$ and -1 occur equally often among all elliptic curves when ordered by height. Indeed, we expect the same to be true in any acceptable family as well.

In this subsection, we prove:

Theorem 37 *Suppose F is an acceptable family of elliptic curves such that exactly 50% of the curves in F, when ordered by height, have root number $+1$. Then at least 25% of the curves in F, when ordered by height, have rank 0. Furthermore, if we assume that all the elliptic curves in F have finite Tate-Shafarevich groups, then at least 41.6% of the curves in F have rank 1.*

We will construct an explicit positive proportion family F satisfying the hypotheses of Theorem 37; this will then imply Theorem 4. (Of course, it is expected that the family F of all curves satisfies the root number hypothesis of the theorem; however, this remains unproved.)

Our proof of Theorem 37 is based on Theorem 26 in conjunction with a recent remarkable result of Dokchitser and Dokchitser [19] which asserts (as predicted by the Birch and Swinnerton-Dyer conjecture) that the parity of the p-Selmer rank of an elliptic curve E (for any prime p) is determined by the root number of E:

Theorem 38 (Dokchitser–Dokchitser) *Let E be an elliptic curve over $\mathbb{Q}$ and let p be any prime. Then the rank of the p-Selmer group of E is even if and only if the root number of E is $+1$.*

We may now prove Theorem 37.

Proof of Theorem 37: By Theorem 26, the average size of the 3-Selmer group of curves in F is at most 4. On the other hand, by Theorem 38 we know that that exactly 50% of the curves in F have odd 3-Selmer rank and thus have at least 3 elements in the 3-Selmer group. Hence the average size of the 3-Selmer groups of the 50% of elliptic curves in F having even 3-Selmer rank is at most 5. Now if the 3-Selmer group of an elliptic curve has even rank, then it must have size 1, 9, or more than 9. For the average of such sizes to be 5, at least half must be equal to 1. Thus among these 50% of curves in F with even 3-Selmer rank, at least half have trivial 3-Selmer group, and therefore have rank 0.

Next, suppose that every odd rank curve in F has a finite Tate-Shafarevich group. A well-known result of Cassels states that if $E/\mathbb{Q}$ is an elliptic curve such that $Ш(E)$ is finite, then $Ш(E)$ is square. Now if the 3-Selmer group of an elliptic curve has odd rank, then it must have size 3, 27, or more than 27. For the average of such sizes to be 7, at least 5/6 of them must equal 3. Thus among these 50% of curves in F with odd 3-Selmer rank, at least 5/6 of them have 3-Selmer group of size 3. Since Ш is always a square, we conclude that Ш[3] for all these elliptic curves is trivial and so they each have rank 1. □

We now construct an explicit positive proportion acceptable family F of elliptic curves in which exactly 50% of the curves have root number equal to 1. By Theorem 37, this will then imply Theorems 4 and 5.

First, recall that the root number $\omega(E)$ of an elliptic curve E over $\mathbb{Q}$ may be expressed in terms of a product over all primes of local root numbers $\omega_p(E)$ of E, namely, $\omega(E) = -\prod_p \omega_p(E)$. The local root number $\omega_p(E)$ is easy to compute when E has good or multiplicative reduction at p. In fact, it is known (see, e.g., [27]) that $\omega_p(E) = 1$ whenever E has good or non-split multiplicative reduction at p, and $\omega_p(E) = -1$ when E has split multiplicative reduction at p.

Suppose an elliptic curve $E/\mathbb{Q}$ has multiplicative reduction at a prime $p \geq 3$. Then it is easily checked that E has split reduction precisely when $\left(\frac{-2J}{p}\right) = 1$. It is also clear that if E_{-1} denotes the twist of E over $\mathbb{Q}[i]$, then $J(E_{-1}) = -J(E)$. Hence, given an odd prime p for which E has multiplicative reduction at p, we have $\omega_p(E) = \omega_p(E_{-1})$ if and only if $p \equiv 1 \pmod 4$.

Let F denote the set of all elliptic curves E over $\mathbb{Q}$ satisfying the following conditions:

- E is semistable;
- E has good reduction at 2;
- $\Delta(E)/9$ is a squarefree integer relatively prime to 3.

The set F is clearly acceptable. Moreover, if $E \in F$, then the twist E_{-1} of E by -1 is also clearly in F, since semistability, good reduction at 2, and discriminant of an elliptic curve are all preserved under such a twist. Because the discriminant of any curve in F is odd, it must be congruent to 1 modulo 4; therefore, the number of primes (counted with multiplicuty) congruent to 3 (mod 4) that divide the discriminant is even. Since the highest power of 3 dividing $\Delta(E)$ is 9 and since $\Delta(E)/9$ is squarefree, the number of distinct primes congruent to 3 (mod 4) that divide the discriminant is odd. Now for a prime factor p of the discriminant, we have already observed that $\omega_p(E) = -\omega_p(E_{-1})$ if and only if $p \equiv 3 \pmod 4$; therefore, $\omega(E) = -\omega(E_{-1})$ for all $E \in F$. Since the height of an elliptic curve also remains the same under twisting by -1, it follows that a density of exactly 50% of elliptic curves in F, when ordered by height, have root number $+1$, as desired.

We have proven Theorems 4 and 5.

4.2 Elliptic curves having analytic rank 0

We may similarly prove that a positive proportion of all elliptic curves have analytic rank 0, by combining our counting arguments with the recent beautiful work of Skinner–Urban [30]. Their work implies, in particular, that if $E/\mathbb{Q}$ is an elliptic curve satisfying certain mild conditions and having trivial 3-Selmer group (and therefore rank 0), then the L-function of E does not vanish at the point 1! The following theorem is a consequence of [30, Theorem 2]:

Theorem 39 (Skinner–Urban) *Let $E/\mathbb{Q}$ be an elliptic curve such that:*

(a) *The 3-Selmer group of E is trivial;*

(b) *E is semistable;*

(c) *E has good ordinary reduction at 3;*

(d) *The action of $G_{\mathbb{Q}}$ on $E[3]$ is irreducible.*

Then $L(E,1) \neq 0$.

We may use Theorem 37 in conjunction with Skinner and Urban's Theorem to prove:

Theorem 40 *Suppose F is an acceptable family of semistable elliptic curves having good ordinary reduction at 3 such that exactly 50% of the curves in F, when ordered by height, have root number $+1$. Then at least 25% of elliptic curves in F have analytic rank 0.*

Proof: It is a consequence of a result of Duke (see [14, Theorem 1]) that 100% of all elliptic curves E, when ordered by height, have the property that the action of $G_{\mathbb{Q}}$ on $E[3]$ is irreducible. As F is an acceptable family, it contains a positive proportion of all elliptic curves, and so 100% of the curves in F satisfy condition (d) of Theorem 39. The proof of Theorem 37 now implies that 25% of the curves in F satisfy all four conditions of Theorem 39, and so the desired result follows. □

As in §4.1, we may construct an explicit positive proportion acceptable family F of elliptic curves satisfying the hypotheses of Theorem 40. Indeed, let F denote the family of all elliptic curves E satisfying the following conditions:

- E is semistable;
- E has good reduction at 2, and both E and E_{-1} have good ordinary reduction at 3;
- $\Delta(E)/49$ is a squarefree integer relatively prime to 7.

Then, just as in §4.1, we see that 50% of the curves in F have root number $+1$. Thus, by Theorem 40, a positive proportion of all elliptic curves, when ordered by height, have both algebraic and analytic rank 0; we have proven Theorem 6 and Corollary 7.

Acknowledgments

We are very grateful to John Cremona, Shrenik Shah, and Chris Skinner for helpful conversations.

References

[1] S. Y. An, S. Y. Kim, D. C. Marshall, S. H. Marshall, W. G. McCallum, and A. R. Perlis, Jacobians of genus one curves, *J. Number Theory* **90** (2001), no. 2, 304–315.

[2] M. Artin, F. Rodriguez-Villegas, and J. Tate, On the Jacobians of plane cubics, *Adv. Math.* **198** (2005), no. 1, 366–382.

[3] B. Bektemirov, B. Mazur, W. Stein, and M. Watkins, Average ranks of elliptic curves: tension between data and conjecture, *Bull. Amer. Math. Soc.* **44** (2007), no. 2, 233–254.

[4] M. Bhargava, The density of discriminants of quartic rings and fields, *Ann. of Math.* **162**, 1031–1063.

[5] M. Bhargava, The density of discriminants of quintic rings and fields, *Ann. of Math.* to appear.

[6] M. Bhargava, Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants, *Int. Math. Res. Not.*, IMRN 2007, no. 17, Art. ID rnm052, 20 pp.

[7] M. Bhargava and A. Shankar, Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves, preprint.

[8] B. J. Birch and H. P. F. Swinnerton-Dyer, Notes on elliptic curves I, *J. Reine Angew. Math.* **212** 1963 7–25.

[9] A. Borel and Harish-Chandra, Arithmetic subgroups of algebraic groups, *Ann. of Math.* **75** (1962), 485–535.

[10] A. Brumer, The average rank of elliptic curves I, *Invent. Math.* **109** (1992), no. 3, 445–472.

[11] A. Brumer and K. Kramer, The rank of elliptic curves, *Duke Math J.* **44** (1977), no. 4, 715–743.

[12] J. W. S. Cassels, Arithmetic on curves of genus 1, IV: Proof of the Hauptvermutung, *J. Reine Angew. Math.* **211** (1962), 95–112.

[13] J. Cremona, T. Fisher, and M. Stoll, Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves, preprint.

[14] W. Duke, Elliptic curves with no exceptional primes, *C. R. Acad. Sci. Paris Sr. I Math.* **325** (1997), no. 8, 813–818.

[15] H. Davenport, On a principle of Lipshitz, *J. London Math. Soc.* **26** (1951), 179–183. Corrigendum: "On a principle of Lipschitz", *J. London Math. Soc.* **39** (1964), 580.

[16] H. Davenport, On the class-number of binary cubic forms I and II, *J. London Math. Soc.* **26** (1951), 183–198.

[17] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields II, *Proc. Roy. Soc. London Ser. A* **322** (1971), no. 1551, 405–420.

[18] L. E. Dickson, A fundamental system of covariants of the ternary cubic form, *Ann. of Math. (2)* **23** (1921), 78–82.

[19] T. Dokchitser and V. Dokchitser, On the Birch–Swinnerton-Dyer quotients modulo squares, preprint.

[20] É Fouvry, Sur le comportement en moyenne du rang des courbes $y^2 = x^3 + k$, Séminaire de Théorie des Nombres, Paris, 1990–91, 61–84, *Prog. Math.* **108**, Birkhauser Boston, Boston, MA, 1993.

[21] C. G. Gibson, Elementary geometry of algebraic curves, Cambridge University Press, Cambridge, 1998.

[22] D. Goldfeld, Conjectures on elliptic curves over quadratic fields, in *Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979)*, 108–118, *Lecture Notes in Math.* **751**, Springer, Berlin, 1979.

[23] D. R. Heath-Brown, The average analytic rank of elliptic curves, *Duke Math. J.* **122** (2004), no. 3, 591–623.

[24] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications **45**, American Mathematical Society, Providence, RI, 1999.

[25] A. W. Knapp, Lie groups beyond an introduction, Second Ed., *Prog. Math.* **140**, Birkhauser Boston, Boston, MA, 2002.

[26] A. Kraus, Quelques remarques à propos des invariants c_4, c_6 et Δ d'une courbe elliptique, *Acta Arith.* **54** (1989), no. 1, 75–80.

[27] D. E. Rohrlich, Variation of the root number in families of elliptic curves, *Compositio Math.* **87** (1993), no. 2, 119–151.

[28] C. L. Siegel, The average measure of quadratic forms with given determinant and signature, *Ann. of Math. (2)* **45** (1944), 667–685.

[29] J. H. Silverman, The arithmetic of elliptic curves, Second Ed., *Graduate Texts in Math.* **106**, Springer-Verlag, 1986.

[30] C. Skinner and E. Urban, The Iwasawa main conjectures for GL_2, in preparation.

[31] G. Solomon, Higher plane curves, Third Ed., 1879, reprinted by Chelsea, NY.

[32] M. P. Young, Low-lying zeros of families of elliptic curves, *J. Amer. Math. Soc.* **19** (2006), no. 1, 205–250.